Schaum

ÁLGEBRA MODERNA

Frank Ayres, Jr.

Mc Graw Hill

ALGEBRA MODERNA

FRANK AYRES, JR., Ph. D.

Formerly Professor and Head,
Department of Mathematics
Dickinson College

TRADUCCION Y ADAPTACION

JESÚS MARÍA CASTAÑO

Profesor de Matemáticas de la Universidad del Valle, Colombia

Con la colaboración de

EMILIO ROBLEDO MONCADA

Profesor del Centro de Estudios Universitarios, Madrid

McGRAW-HILL

MÉXICO • BUENOS AIRES • CARACAS • GUATEMALA • LISBOA • MADRID • NUEVA YORK
SAN JUAN • SANTAFÉ DE BOGOTÁ • SANTIAGO • SÃO PAULO • AUCKLAND
LONDRES • MILÁN • MONTREAL • NUEVA DELHI • SAN FRANCISCO • SINGAPUR
ST. LOUIS • SIDNEY • TORONTO

ÁLGEBRA MODERNA

Atlacomulco 499-501, Fracc. Ind. San Andrés Atoto
53500 Naucalpan de Juárez, Edo. de México
Miembro de la Cámara Nacional de la Industria Editorial, Reg. Núm. 1890

ISBN 968-422-917-8

Traducido de la primera edición en Inglés de
SCHAUM'S OUTLINE OF MODERN ALGEBRA
Copyright © MCMLXV, by McGraw-Hill, Inc. U.S.A
ISBN 0-07-091522-9

1302456789 09876542103

Impreso en México Printed in Mexico

Esta obra se terminó de
Imprimir en Septiembre del 2003
Programas Educativos S.A de C.V.
Calz. Chabacano No. 65-A
Col. Asturias C.P. 06850 México D.F.
Empresa certificada por el Instituto Mexicano
de Normalización y Certificado A.C. Bajo la
Norma ISO-9002, 1994/NMX-CC-04 1995 con
el núm.de registro RSC-048 y bajo la Norma
ISO-14001:1996/SAA-1998, con el núm.de
registro RSAA-003.

Prólogo

Este libro, dedicado al estudio de sistemas algebraicos, tiene por fin servir de complemento a los textos corrientes o bien ser utilizado como texto, por si solo, en cursos de álgebra abstracta moderna a nivel medio y superior. Como tal, su propósito, más que ofrecer un estudio en profundidad de uno o más sistemas algebraicos, es proporcionar sólidos fundamentos para el ulterior estudio de toda una serie de ellos.

En los dos primeros capítulos se trata de los componentes fundamentales de los sistemas algebraicos —conjuntos de elementos, relaciones, operaciones, aplicaciones—. El plan del libro ha quedado así establecido.

1) presentación concisa del tema,
2) amplia variedad de ejemplos,
3) demostraciones de la mayoría de los teoremas entre los problemas resueltos,
4) una serie de ejercicios propuestos cuidadosamente escogida.

El Capítulo 3 comienza con los postulados de Peano para los números naturales, a los que sigue la interpretación de los diversos sistemas de números algebraicos y se completa con la deducción de sus propiedades más sobresalientes. Siguiendo este orden de exposición no solamente se introduce al lector en el desarrollo detallado y riguroso de estos sistemas de números, sino que se le provee de la práctica necesaria para la deducción de propiedades de los sistemas abstractos que siguen a continuación.

El primer sistema algebraico —el grupo— se estudia en el Capítulo 9. Se examinan las clases laterales según un subgrupo, los subgrupos invariantes y sus grupos cocientes; y el capítulo termina con el teorema de Jordan-Hölder para grupos finitos.

Los Capítulos 10-11 tratan de los anillos, dominios de integridad y cuerpos. A continuación, en el Capítulo 12, se estudian los polinomios sobre anillos y cuerpos a la vez que algunos conceptos de la teoría elemental de ecuaciones. En todos estos capítulos se presta mucha atención a los anillos finitos.

El Capítulo 13 trata de los espacios vectoriales. El álgebra de las transformaciones lineales en un espacio vectorial de dimensión finita conduce naturalmente al álgebra de matrices (Capítulo 14). Las matrices se emplean, pues, para resolver sistemas de ecuaciones lineales y proporcionar así soluciones más simples a ciertos problemas relacionados con los espacios vectoriales. En el Capítulo 15 se tratan los polinomios de matrices como un ejemplo de anillo de polinomios no conmutativo. Se define luego el polinomio característico de una matriz cuadrada sobre un cuerpo. Las raíces características y los vectores invariantes asociados de las matrices simétricas reales se utilizan para reducir las ecuaciones de las cónicas y de las superficies cuádricas a la forma canónica. En el Capítulo 16 se definen formalmente las álgebras lineales y se consideran brevemente otros ejemplos.

En el capítulo final se exponen las álgebras booleanas y se indican las importantes aplicaciones que tienen en circuitos eléctricos simples.

El autor aprovecha esta oportunidad para expresar su agradecimiento al personal de la Schaum Publishing Company, en especial a Jeffrey Albert y a Alan Hopenwasser, por su cooperación incondicional.

FRANK AYRES, JR.

Tabla de materias

TABLA DE MATERIAS

Capítulo 1

Conjuntos

CONJUNTOS

Cualquier colección de objetos como (*a*) los puntos de un segmento dado, (*b*) las rectas que pasan por un punto en el espacio ordinario, (*c*) los números naturales menores que diez, (*d*) los cinco chicos Rodríguez y su perro, (*e*) las páginas de este libro..., se dice un *conjunto* o *clase*. Los puntos, las rectas, los números, los chicos y el perro, las páginas..., se dirán *elementos* de los conjuntos respectivos. Por lo general, los conjuntos se denotan con letras mayúsculas y los elementos cualesquiera de los conjuntos se denotan con minúsculas.

Sea A un conjunto dado y sean p y q ciertos objetos. Si p es un elemento de A, se indicará esto escribiendo $p \in A$; si tanto p como q son elementos de A, se escribirá $p, q \in A$ en vez de $p \in A$ y $q \in A$; cuando q no es elemento de A, se escribe $q \notin A$.

Si bien en gran parte de nuestro estudio no tendrá nada que ver el tipo de los elementos, en muchos de los ejemplos y problemas aparecen naturalmente conjuntos de números. Por comodidad, se reservan desde ahora,

N para denotar el conjunto de todos los números naturales
Z para denotar el conjunto de todos los enteros
Q para denotar el conjunto de todos los números racionales
R para denotar el conjunto de todos los números reales

Ejemplo 1:

(*a*) $1 \in N$ y $205 \in N$ puesto que 1 y 205 son números naturales; $\frac{1}{2}, -5 \notin N$ ya que $\frac{1}{2}$ y -5 no son números naturales.

(*b*) El símbolo $\in$ indica pertenencia y puede leerse «en», «está en», «están en», «elemento de» según el contexto. Así, «Sea $r \in Q$» puede leerse como «Sea r elemento de Q»; y «Para cualesquiera $p, q \in Z$» se puede leer «Para cualesquiera p y q en Z». Escribiremos a veces $n \neq 0 \in Z$ en vez de $n \neq 0, n \in Z$; también $p \neq 0, q \in Z$ en vez de $p, q \in Z$ con $p \neq 0$.

Los conjuntos que se van a introducir aquí serán siempre *bien definidos*, esto es, que siempre será posible determinar si un objeto dado pertenece o no a un cierto conjunto. Los conjuntos del primer párrafo vienen definidos por enunciados precisos en palabras. A veces se da un conjunto en forma tabular, escribiendo sus elementos entre llaves, por ejemplo:

$A = \{a\}$ es el conjunto que consta del solo elemento a.
$B = \{a, b\}$ es el conjunto que consta de los elementos a y b.
$C = \{1, 2, 3, 4\}$ es el conjunto de números naturales menores que 5.
$K = \{2, 4, 6, \ldots\}$ es el conjunto de todos los números naturales pares.
$L = \{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\}$ es el conjunto de todos los enteros divisibles por 5.

Los conjuntos C, K y L, dados antes, se pueden definir también como sigue:

$C = \{x: x \in N, x < 5\}$
$K = \{x: x \in N, x \text{ es par}\}$
$L = \{x: x \in Z, x \text{ es divisible por } 5\}$

Aquí cada conjunto consiste en *todos* los objetos x que satisfacen las condiciones que siguen a los dos puntos.

Véase Problema 1.

Conjuntos iguales

Cuando dos conjuntos A y B constan de los mismos elementos, se dicen *iguales* y escribiremos $A = B$. Para indicar que A y B no son iguales, escribiremos $A \neq B$.

Ejemplo 2: (i) Si $A = \{\text{María, Elena, Juan}\}$ y $B = \{\text{Elena, Juan, María}\}$, entonces $A = B$. Obsérvese que una variación del orden en que se presentan los elementos de un conjunto no tiene influencia.

(ii) Si $A = \{2, 3, 4\}$ y $B = \{3, 2, 3, 2, 4\}$, es $A = B$, pues cada elemento de A está en B y cada elemento de B está en A. Obsérvese que un conjunto no se altera por que se repitan uno o más elementos suyos.

(iii) Si $A = \{1, 2\}$ y $B = \{1, 2, 3, 4\}$, entonces $A \neq B$ porque 3 es elemento de B pero no de A.

SUBCONJUNTOS DE UN CONJUNTO

Sea S un conjunto dado. Se dice de cualquier conjunto A cada uno de cuyos elementos es también elemento de S, que está *contenido en* S y se le llama *subconjunto* de S.

Ejemplo 3: Los conjuntos $A = \{2\}$, $B = \{1, 2, 3\}$ y $C = \{4, 5\}$ son subconjuntos del $S = \{1, 2, 3, 4, 5\}$. También $D = \{1, 2, 3, 4, 5\} = S$ es subconjunto de S.

El conjunto $E = \{1, 2, 6\}$ no es subconjunto de S puesto que $6 \in E$ pero $6 \notin S$.

Sea A un subconjunto de S. Si $A \neq S$, se dice que A es un *subconjunto propio de* S y se escribe $A \subset S$ (léase «A es subconjunto propio de S», o bien «A está propiamente contenido en S»). Más frecuentemente, y en particular cuando no se excluye la posibilidad $A = S$, escribiremos $A \subseteq S$ (léase «A es subconjunto de S» o bien «A está contenido en S»). De todos los subconjuntos de un conjunto dado S, solamente S mismo es impropio, es decir, no es subconjunto propio de S.

Ejemplo 4: Para los conjuntos del Ejemplo 3 se puede escribir $A \subseteq S$, $B \subseteq S$, $C \subseteq S$, $D \subseteq S$, $E \not\subseteq S$. Los enunciados precisos son, desde luego, $A \subset S$, $B \subset S$, $C \subset S$, $D = S$, $E \not\subseteq S$.

Nótese bien que $\in$ vincula un elemento y un conjunto, en tanto que $\subset$ y $\subseteq$ vinculan dos conjuntos. Así, $2 \in S$ y $\{2\} \subset S$ son enunciados correctos, pero $2 \subset S$ y $\{2\} \in S$ no lo son.

Sea A un subconjunto propio de S. S contiene, pues, los elementos de A junto con ciertos elementos que no están en A. Todos estos últimos elementos, o sea los que no están en A, constituyen otro subconjunto propio de S que se llama *complemento* del subconjunto A en S.

Ejemplo 5: Para el conjunto $S = \{1, 2, 3, 4, 5\}$ del Ejemplo 3, el complemento de $A = \{2\}$ en S es $F = \{1, 3, 4, 5\}$. Asimismo, $B = \{1, 2, 3\}$ y $C = \{4, 5\}$ son subconjuntos complementarios en S.

En nuestra discusión de los subconjuntos complementarios de un conjunto dado se da por sentado que estos subconjuntos son propios. La razón es que, hasta aquí, hemos estado dependiendo de la intuición en lo que respecta a los conjuntos; es decir, que hemos supuesto tácitamente que todo conjunto debe tener al menos un elemento. Para librarnos de esta restricción (y también para que el subconjunto impropio S de S tenga complemento) introducimos el conjunto *vacío* o *nulo* $\varnothing$ como el conjunto que carece de elementos. Se sigue fácilmente que

(i) $\varnothing$ es subconjunto de todo conjunto S.

(ii) $\varnothing$ es subconjunto propio de todo conjunto $S \neq \varnothing$.

Ejemplo 6: Los subconjuntos de $S = \{a, b, c\}$ son: $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$, $\{a, b, c\}$ y $\varnothing$.

Los pares de subconjuntos complementarios son:

$$\{a, b, c\} \text{ y } \varnothing \qquad \{a, b\} \text{ y } \{c\}$$
$$\{a, c\} \text{ y } \{b\} \qquad \{b, c\} \text{ y } \{a\}$$

Hay un número par de subconjuntos y, por tanto, un número impar de subconjuntos propios de un conjunto de 3 elementos. ¿Es esto cierto para un conjunto de 303 elementos? ¿De 303 000 elementos?

CONJUNTOS UNIVERSALES

Si $U \neq \varnothing$ es un cierto conjunto cuyos subconjuntos están en consideración, suele decirse que el conjunto dado es un *conjunto universal*.

Ejemplo 7: Sea la ecuación

$$(x + 1)(2x - 3)(3x + 4)(x^2 - 2)(x^2 + 1) = 0$$

cuyo conjunto solución, es decir, el conjunto cuyos elementos son las raíces de la ecuación, es $S = \{-1, 3/2, -4/3, \sqrt{2}, -\sqrt{2}, i, -i\}$ si el conjunto universal es el conjunto de los números complejos. No obstante, si el conjunto universal es $\mathbb{R}$, el conjunto solución es $A = \{-1, 3/2, -4/3, \sqrt{2}, -\sqrt{2}\}$. ¿Cuál es el conjunto solución si el conjunto universal es Q? ¿Si es Z? ¿Si es N?

Si, por el contrario, se nos dan dos conjuntos $A = \{1, 2, 3\}$ y $B = \{4, 5, 6, 7\}$ y nada más, sabemos poco del conjunto universal U del cual aquéllos son subconjuntos. Por ejemplo, U podría ser $\{1, 2, 3, \ldots, 7\}$, $\{x: x \in N, x \leq 1000\}$, N, Z, ... No obstante, cuando se trata de ciertos conjuntos $A, B, C, \ldots$, siempre los consideraremos como subconjuntos de cierto conjunto universal U no necesariamente definido de manera explícita. Con respecto a este conjunto universal, los complementos de los subconjuntos $A, B, C, \ldots$, se denotarán $A', B', C', \ldots$, respectivamente.

INTERSECCION Y UNION DE CONJUNTOS

Sean A y B conjuntos dados. El conjunto de todos los elementos que pertenecen tanto a A como a B se llama *intersección* de A y B. Se le denotará por $A \cap B$ (léase «intersección de A y B» o bien «A intersección B», o aún «A inter B»). Así, pues,

$$A \cap B = \{x: x \in A \text{ y } x \in B\}$$

El conjunto de todos los elementos que pertenecen ya a A, ya a B, ya a ambos A y B se llama *unión* de A y B. Se le denota por $A \cup B$ (léase «unión de A y B», o bien «A unión B»). Así que,

$$A \cup B = \{x: x \in A \text{ o } x \in B \text{ o } x \in A \cap B\}$$

Escribiremos más a menudo, sin embargo,

$$A \cup B = \{x: x \in A \text{ o } x \in B\}$$

Que da lo mismo, ya que todo elemento de $A \cap B$ lo es de A.

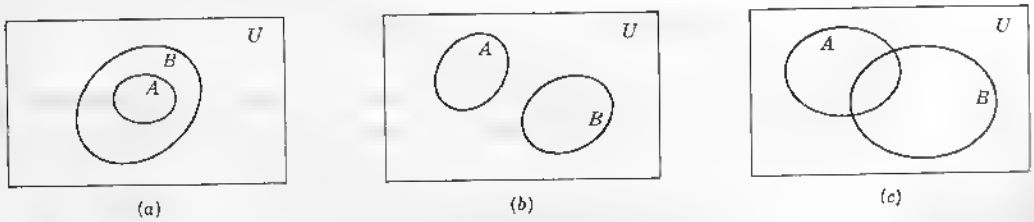
Ejemplo 8: Sean $A = \{1, 2, 3, 4\}$ y $B = \{2, 3, 5, 8, 10\}$; entonces $A \cup B = \{1, 2, 3, 4, 5, 8, 10\}$ y $A \cap B = \{2, 3\}$.

Véanse también los Problemas 2-4.

Dos conjuntos A y B se llaman *disjuntos* si no tienen ningún elemento común, es decir, si $A \cap B = \varnothing$. En el Ejemplo 6, cada dos de los conjuntos $\{a\}$, $\{b\}$, $\{c\}$ son disjuntos; asimismo, los conjuntos $\{a, b\}$ y $\{c\}$, los $\{a, c\}$ y $\{b\}$ y los conjuntos $\{b, c\}$ y $\{a\}$ son disjuntos.

DIAGRAMAS DE VENN

Complemento, intersección y unión se pueden representar mediante los diagramas de Venn. En los diagramas de abajo el conjunto universal U está representado por puntos (que no se indican) en el interior de un rectángulo y cualquiera de sus subconjuntos no vacíos por puntos dentro de las curvas cerradas. (Para evitar confusión, convendremos en que ningún elemento de U está representado por un punto del contorno de alguna de estas curvas.) En la Fig. 1-1(*a*), los subconjuntos A y B de U son tales, que $A \subset B$; en la Fig. 1-1(*b*), $A \cap B = \varnothing$; en la Fig. 1-1(*c*), A y B tienen al menos un elemento común, de modo que $A \cap B \neq \varnothing$.



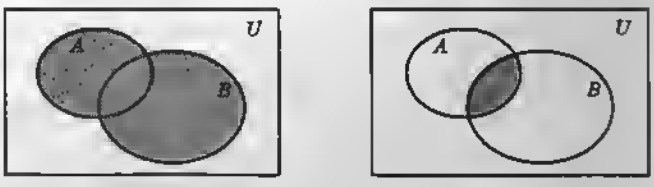
(*a*) (*b*) (*c*)

Fig. 1-1

Supóngase ahora que en el diagrama anterior se sombrea el interior de U exceptuando el interior de A. En cada caso, el área sombreada representará el conjunto complementario A' de A en U.

La unión $A \cup B$ y la intersección $A \cap B$ de los conjuntos A y B de la Fig. 1-1(*c*) se representan por el área sombreada en las Figs. 1-2(*a*) y (*b*), respectivamente. En la Fig. 1-2(*a*), el área no sombreada representa $(A \cup B)'$, complemento de $A \cup B$ en U; en la Fig. 1-2(*b*), el área no sombreada representa $(A \cap B)'$. De estos diagramas, como también de las definiciones de $\cup$ y $\cap$, se desprende claramente que $A \cup B = B \cup A$ y $A \cap B = B \cap A$.

Véanse Problemas 5-7.



(*a*) (*b*)

Fig. 1-2

OPERACIONES CON CONJUNTOS

Además de la complementación, unión e intersección, que llamaremos operaciones con conjuntos, definimos:

La *diferencia* $A - B$, en ese orden, de dos conjuntos A y B es el conjunto de todos los elementos de A que no pertenecen a B, esto es,

$$A - B = \{x: x \in A, x \notin B\}$$

En la Fig. 1-3, $A - B$ se representa por el área sombreada y $B - A$ por el área de doble rayado. De aquí se sigue

$A - B = A \cap B' = B' - A$
$A - B = \varnothing$ si, y solo si, $A \subseteq B$
$A - B = B - A$ si, y solo si, $A = B$
$A - B = A$ si, y solo si, $A \cap B = \varnothing$

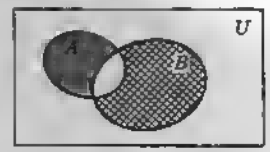


Fig. 1-3

Ejemplo 9: Demostrar: (*a*) $A - B = A \cap B' = B' - A'$; (*b*) $A - B = \varnothing$ si, y solamente si, $A \subseteq B$; (*c*) $A - B = A$ si, y solamente si, $A \cap B = \varnothing$.

(*a*) $A - B = \{x: x \in A, x \notin B\} = \{x: x \in A \text{ y } x \in B'\} = A \cap B'$
$= \{x: x \notin A', x \in B'\} = B' - A'$

(*b*) Supóngase $A - B = \varnothing$. Entonces, por (*a*), $A \cap B' = \varnothing$, esto es, A y B' son disjuntos. Ahora bien, B y B' son disjuntos; luego, como $B \cup B' = U$, se tiene $A \subseteq B$.

Recíprocamente, supóngase $A \subseteq B$. Entonces $A \cap B' = \varnothing$, y $A - B = \varnothing$.

(*c*) Supóngase $A - B = A$. Entonces $A \cap B' = A$, esto es, $A \subseteq B'$. Luego, por (*b*),

$$A \cap (B') = A \cap B = \varnothing$$

Recíprocamente, supóngase $A \cap B = \varnothing$. Entonces $A - B' = \varnothing$, $A \subseteq B'$, $A \cap B' = A$ y $A - B = A$.

En los Problemas 5-7 se han empleado diagramas de Venn para ilustrar algunas propiedades de las operaciones con conjuntos. Por ejemplo, la Fig. 1-3 sugiere que

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

Hay que entender, no obstante, que si bien cualquier teorema o propiedad se puede ilustrar con un diagrama de Venn, ningún teorema se puede demostrar con el diagrama.

Ejemplo 1u: Demostrar: $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$.

La demostración consiste en probar que todo elemento de $(A - B) \cup (B - A)$ es elemento de $(A \cup B) - (A \cap B)$ y, recíprocamente, que todo elemento de $(A \cup B) - (A \cap B)$ es elemento de $(A - B) \cup (B - A)$. Cada paso se da a partir de una definición previa y se deja al lector la justificación de ellos.

Sea $x \in (A - B) \cup (B - A)$; entonces $x \in A - B$ o bien $x \in B - A$. Si $x \in A - B$, se sigue que $x \in A$ pero $x \notin B$; si $x \in B - A$, es $x \in B$ pero $x \notin A$. En cualquier caso, $x \in A \cup B$ pero $x \notin A \cap B$. Luego, $x \in (A \cup B) - (A \cap B)$ y

$$(A - B) \cup (B - A) \subseteq (A \cup B) - (A \cap B)$$

Recíprocamente, sea $x \in (A \cup B) - (A \cap B)$; entonces $x \in A \cup B$ pero $x \notin A \cap B$. Ahora bien, o es $x \in A$ pero $x \notin B$, es decir $x \in A - B$, o bien $x \in B$ pero $x \notin A$, es decir, $x \in B - A$. Por tanto, $x \in (A - B) \cup (B - A)$ y $(A \cup B) - (A \cap B) \subseteq (A - B) \cup (B - A)$.

Por último, $(A - B) \cup (B - A) \subseteq (A \cup B) - (A \cap B)$ y $(A \cup B) - (A \cap B) \subseteq (A - B) \cup (B - A)$ implican $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$.

Para referencia posterior, damos aquí una lista de las leyes más importantes que rigen las operaciones con conjuntos. Aquí, los conjuntos A, B, C son subconjuntos de U, el conjunto universal.

LEYES DE OPERACIONES CON CONJUNTOS			
(1.1)	$(A')' = A$		
(1.2)	$\emptyset' = U$	(1.2')	$U' = \emptyset$
(1.3)	$A - A = \emptyset, \quad A - \emptyset = A, \quad A - B = A \cap B'$		
(1.4)	$A \cup \emptyset = A$	(1.4')	$A \cap U = A$
(1.5)	$A \cup U = U$	(1.5')	$A \cap \emptyset = \emptyset$
(1.6)	$A \cup A = A$	(1.6')	$A \cap A = A$
(1.7)	$A \cup A' = U$	(1.7')	$A \cap A' = \emptyset$
	Leyes asociativas		
(1.8)	$(A \cup B) \cup C = A \cup (B \cup C)$	(1.8')	$(A \cap B) \cap C = A \cap (B \cap C)$
	Leyes conmutativas		
(1.9)	$A \cup B = B \cup A$	(1.9')	$A \cap B = B \cap A$
	Leyes distributivas		
(1.10)	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	(1.10')	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
	Leyes de De Morgan		
(1.11)	$(A \cup B)' = A' \cap B'$	(1.11')	$(A \cap B)' = A' \cup B'$
(1.12)	$A - (B \cup C) = (A - B) \cap (A - C)$	(1.12')	$A - (B \cap C) = (A - B) \cup (A - C)$

Véanse Problemas 8-16.

CONJUNTO PRODUCTO

Sean $A = \{a, b\}$ y $B = \{b, c, d\}$. El conjunto de pares ordenados distintos

$$C = \{(a, b),\ (a, c),\ (a, d),\ (b, b),\ (b, c),\ (b, d)\}$$

en que el primer componente de cada par es un elemento de A en tanto que el segundo es un elemento de B, se llama *conjunto producto* $C = A \times B$ (en ese orden) de los conjuntos dados. Así que, si A y B son conjuntos cualesquiera, definimos

$$A \times B = \{(x, y) : x \in A, y \in B\}$$

Ejemplo 11: Identificar los elementos de $X = \{1, 2, 3\}$ como coordenadas de puntos sobre el eje x (véase Fig. 1-4) considerado como escala numérica, y los elementos de $Y = \{1, 2, 3, 4\}$ como coordenadas de puntos sobre el eje y considerado como escala numérica. Entonces los elementos de $X \times Y$ son las coordenadas rectangulares de los 12 puntos indicados. De igual manera, si $X = Y = N$, el conjunto $X \times Y$ es el de las coordenadas de todos los puntos del primer cuadrante que tienen coordenadas naturales.

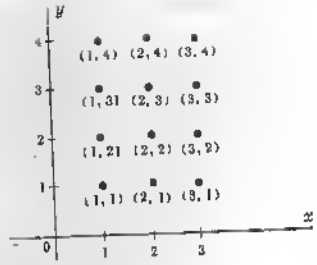


Fig. 1-4

APLICACIONES

Considérese el conjunto $H = \{h_1, h_2, h_3, \ldots, h_8\}$ de todas las casas de una manzana que dan a la calle Mayor y el conjunto $C = \{c_1, c_2, c_3, \ldots, c_{39}\}$ de todos los niños que viven en la manzana en dicha calle. Parece natural asociar cada niño de C con la casa de H en la cual vive ese niño. Supongamos que se tiene así asociados c_1 con h_2, c_2 con h_5, c_3 con h_2, c_4 con h_5, c_5 con h_8, $\ldots$, c_{39} con h_3. Una asociación semejante de elementos o correspondencia entre elementos de C y H se dice *aplicación* de C en H. El elemento único de H asociado con cualquier elemento de C se llama *imagen* de aquel elemento (de C) en la aplicación.

Se presentan dos posibilidades en esta aplicación: (1) todo elemento de H es imagen, esto es, en cada casa vive por lo menos un niño; (2) al menos un elemento de H no es imagen, es decir, al menos en una casa no viven niños. En el caso (1) diremos que la correspondencia es una *aplicación sobreyectiva* de C en H, o que se trata de una *sobreyección de C en H* o bien, simplemente, que se tiene una *aplicación C sobre H*. Así, pues, la presencia del «sobre» indica que en la aplicación todo elemento de H es imagen. En el caso (2), se dice que la correspondencia es una aplicación de *C en H* simplemente, pero cuando se dice que «α es una aplicación de A en B» no se excluye la posibilidad de que α sea efectivamente una aplicación de *A sobre B*. Solo cuando se precise distinguir entre dichos casos habrá que escribir «α es una aplicación de A sobre B» o bien «α es una aplicación de A en B, pero no sobre B».

Una aplicación α de un conjunto en otro se puede definir de varias maneras. Por ejemplo, la aplicación de C en H anterior se puede definir enumerando los pares ordenados

$$\alpha = \{(c_1, h_2),\ (c_2, h_5),\ (c_3, h_2),\ (c_4, h_5),\ (c_5, h_8),\ \ldots,\ (c_{39}, h_3)\}$$

Se ve ahora claro que α es simplemente un cierto subconjunto del conjunto producto $C \times H$ de C y H. Así que definimos:

> Una aplicación de un conjunto A en un conjunto B es un subconjunto de $A \times B$, en el cual cada elemento de A aparece una vez, y solo una vez, como primer componente en los elementos del subconjunto.

En toda aplicación α de A en B, el conjunto A se llama *dominio de definición* y el conjunto B se llama *codominio* de α. Si la aplicación es sobreyectiva, B se llama también *dominio de imágenes* de α; en otro caso, el dominio de imágenes de α es el subconjunto propio de B formado por las imágenes de todos los elementos de A.

Una aplicación de un conjunto A en un conjunto B también se puede poner de manifiesto mediante una flecha $\rightarrow$ que vincule los elementos asociados.

Ejemplo 12: Sean $A = \{a, b, c\}$ y $B = \{1, 2\}$. Entonces

$$\alpha:\ a \rightarrow 1,\ b \rightarrow 2,\ c \rightarrow 2$$

es una aplicación de A sobre B (cada elemento de B es imagen), en tanto que

$$\beta:\ 1 \rightarrow a,\ 2 \rightarrow b$$

es una aplicación de B en A, pero no sobre A (no todo elemento de A es imagen).

En la aplicación α, A es el dominio de definición y B es el codominio y también el dominio de imágenes. En la aplicación β, B es el dominio de definición, A es el codominio y $C = \{a, b\} \subset A$ es el dominio de imágenes.

Si es corto el número de elementos que intervienen, se pueden utilizar ventajosamente los diagramas de Venn. La Fig. 1-5 muestra las aplicaciones α y β de este ejemplo.

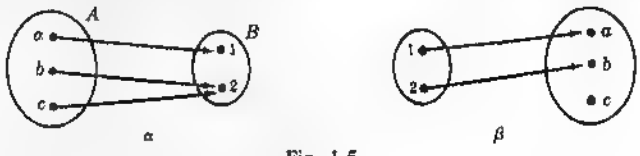


Fig. 1-5

Una tercera manera de denotar una aplicación viene en el

Ejemplo 13: Considérese la aplicación α de N en sí mismo, es decir, de N en N,

$$\alpha: \quad 1 \to 3,\ 2 \to 5,\ 3 \to 7,\ 4 \to 9,\ \ldots$$

o más brevemente,

$$\alpha: \quad n \to 2n + 1,\ n \in N$$

Una aplicación semejante se definirá con frecuencia así:

$$\alpha: \quad 1\alpha = 3,\ 2\alpha = 5,\ 3\alpha = 7,\ 4\alpha = 9,\ \ldots$$

o más brevemente,

$$\alpha: \quad n\alpha = 2n + 1,\ n \in N$$

Aquí es N el dominio de definición (también es el codominio), pero no es el dominio de imágenes de la aplicación. Este es el subconjunto propio M de N dado por

$$M = \{x:\ x = 2n + 1,\ n \in N\}$$

o bien

$$M = \{x:\ x \in N,\ x \text{ impar}\}$$

Las aplicaciones de un conjunto X en un conjunto Y, especialmente cuando X y Y son conjuntos de números, son mejor conocidas del lector como *funciones*. Por ejemplo, definiendo $X = N$ y $Y = M$ en el Ejemplo 13 y empleando f en vez de α, la aplicación (función) se puede expresar en *notación funcional como*

$$\text{(i)} \qquad y = f(x) = 2x + 1$$

Se dice que aquí y está definida como *función de* x. Hoy es usual distinguir entre «función» y «función de». Así, en el ejemplo, definiríamos la función f por

$$f = \{(x, y):\ y = 2x + 1,\ x \in X\}$$

o bien

$$f = \{(x,\ 2x + 1):\ x \in X\}$$

o sea como el subconjunto particular de $X \times Y$ determinado por la «regla» (i), considerando ésta como tal. En gran parte de este libro diremos mejor aplicación que función y así se utilizará poco la notación funcional.

Sea α una aplicación de A en B y sea β una aplicación de B en C. Así, pues, el efecto de α es aplicar $a \in A$ en $a\alpha \in B$ y el efecto de B es aplicar $a\alpha \in B$ en $(a\alpha)\beta \in C$. El resultado final de aplicar α y en seguida β es una aplicación de A en C que definimos por

$$\alpha\beta: \quad a(\alpha\beta) = (a\alpha)\beta,\ a \in A$$

Diremos que $\alpha\beta$ es el *producto de composición* de las aplicaciones α y β en ese orden, o que es la aplicación compuesta de α y β. Desafortunadamente, la notación no está todavía normalizada, de manera que $\alpha\beta$ se utiliza a veces para denotar el efecto de la aplicación β seguido de la aplicación α.

Ejemplo 14: Sea $A = \{a, b, c\}$, $B = \{d, e\}$, $C = \{f, g, h, i\}$ y

$$\alpha: \quad a\alpha = d, \quad b\alpha = e, \quad c\alpha = e$$

$$\beta: \quad d\beta = f, \quad e\beta = h$$

Entonces, $\alpha\beta$: $a(\alpha\beta) = (a\alpha)\beta = d\beta = f$, $b(\alpha\beta) = e\beta = h$, $c(\alpha\beta) = h$

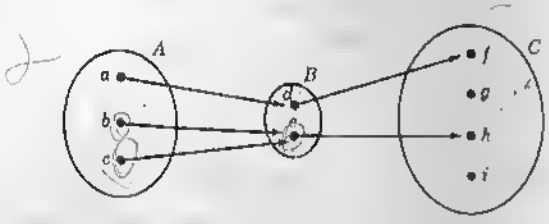


Fig. 1-6

APLICACIONES INYECTIVAS Y BIYECTIVAS

Una aplicación $a \to a'$ de un conjunto A en un conjunto B, se dice *aplicación inyectiva* de A en B, o *inyección* de A en B, si las imágenes de elementos diferentes de A son elementos distintos de B; si, además, cada elemento de B es imagen, o sea, si la aplicación es también sobreyectiva, se dice que esta aplicación es *biyectiva*, o que es una *biyección* de A sobre B o *biyección entre* los dos conjuntos. Anteriormente solía decirse que la aplicación era una *correspondencia biunívoca* entre los conjuntos A y B; esto es claro, pues la aplicación $a \to a'$ induce una aplicación $a' \to a$ de B sobre A y se pueden combinar ambas aplicaciones en la forma $a \leftrightarrow a'$.

Ejemplo 15:

(*a*) La aplicación α del Ejemplo 14 no es una biyección de A en B (los elementos b y c, diferentes, de A, tienen la misma imagen).

(*b*) La aplicación β del Ejemplo 14 es una inyección de B en C, pero no es sobreyección ($g \in C$ no es imagen).

(*c*) Si $A = \{a, b, c, d\}$ y $B = \{p, q, r, s\}$.

$$\text{(i)} \quad \alpha_1: \quad a \leftrightarrow p, \ b \leftrightarrow q, \ c \leftrightarrow r, \ d \leftrightarrow s$$

y

$$\text{(ii)} \quad \alpha_2: \quad a \leftrightarrow r, \ b \leftrightarrow p, \ c \leftrightarrow q, \ d \leftrightarrow s$$

son ejemplos de aplicaciones biyectivas entre A y B.

Se dice que dos conjuntos A y B tienen el mismo número de elementos si, y solamente si, existe una biyección entre A y B. Se dice que un conjunto A tiene n elementos si hay una biyección entre A y el subconjunto $S = \{1, 2, 3, \ldots, n\}$ de N. En este caso, se dice que A es un *conjunto finito*.

La aplicación $\alpha: \quad n\alpha = 2n, \ n \in N$

de N sobre el subconjunto propio $M = \{x: x \in N, x \text{ es par}\}$ de N es inyectiva y sobreyectiva, pero ahora N es un *conjunto infinito*; así que se puede definir un conjunto infinito como el conjunto aplicable biyectivamente en un subconjunto propio suyo; es decir, entre un conjunto infinito y un subconjunto propio del mismo puede haber una biyección.

Se dice que un conjunto infinito es *enumerable* si hay biyección entre ese conjunto y el conjunto N de los números naturales.

BIYECCION DE UN CONJUNTO SOBRE SI MISMO

Sean $\alpha: x \leftrightarrow x + 1$, $\beta: x \leftrightarrow 3x$, $\gamma: x \leftrightarrow 2x - 5$, $\delta: x \leftrightarrow x - 1$

aplicaciones biyectivas de R sobre sí mismo. Como para todo $x \in R$

$$x\alpha\beta = (x+1)\beta = 3(x+1)$$

en tanto que $$x\beta\alpha = (3x)\alpha = 3x + 1$$

vemos que (i) $$\alpha\beta \neq \beta\alpha$$

No obstante, $$x\gamma\delta = (2x-5)\delta = 2x - 6$$

y $$x\alpha(\gamma\delta) = (x+1)\gamma\delta = 2(x+1) - 6 = 2x - 4$$

en tanto que $$x\alpha\gamma = (x+1)\gamma = 2x - 3$$

y $$x(\alpha\gamma)\delta = (2x-3) - 1 = 2x - 4$$

Así, pues, (ii) $$\alpha(\gamma\delta) = (\alpha\gamma)\delta$$

Ahora bien, $$x\alpha\delta = (x+1)\delta = x$$

y $$x\delta\alpha = (x-1)\alpha = x$$

o sea, que α seguida de δ (o también, δ seguida de α) aplica cada $x \in R$ en sí mismo. Denotando por $\mathcal{I}$ la aplicación *idéntica* (neutra),

$$\mathcal{I}: x \leftrightarrow x$$

Así que (iii) $$\alpha\delta = \delta\alpha = \mathcal{I}$$

es decir, que δ anula el efecto de α (o también, α anula el de δ). En vista de (iii), δ se llama *aplicación recíproca* de α y se escribe $\delta = \alpha^{-1}$; también es α la recíproca de δ y se escribe $\alpha = \delta^{-1}$.

Véase Problema 18.

En el Problema 19 se demuestra el

Teorema I. Si α es una aplicación biyectiva de un conjunto S sobre un conjunto T, α tiene entonces una recíproca única, y al contrario.

En el Problema 20 se demuestra el

Teorema II. Si α es una aplicación biyectiva de un conjunto S sobre un conjunto T, y β es una aplicación biyectiva de T sobre un conjunto U, entonces es $(\alpha\beta)^{-1} = \beta^{-1} \cdot \alpha^{-1}$.

Problemas resueltos

1. Mostrar en forma tabular (*a*) $A = \{a: a \in N, 2 < a < 6\}$, (*b*) $B = \{p: p \in N, p < 10, p \text{ es par}\}$, (*c*) $C = \{x: x \in Z, 2x^2 + x - 6 = 0\}$.

(*a*) Aquí A consta de todos los números naturales ($a \in N$) entre 2 y 6; así, pues, $A = \{3, 4, 5\}$.

(*b*) B consiste en los números naturales impares menores que 10; de modo que $B = \{1, 3, 5, 7, 9\}$.

(*c*) Los elementos de C son las raíces enteras de $2x^2 + x + 6 = (2x - 3)(x + 2) = 0$; así que $C = \{-2\}$.

2. Sean $A = \{a, b, c, d\}$, $B = \{a, c, g\}$, $C = \{c, g, m, n, p\}$. Hallar:

$A \cup B = \{a, b, c, d, g\}$, $A \cup C = \{a, b, c, d, g, m, n, p\}$, $B \cup C = \{a, c, g, m, n, p\}$;
$A \cap B = \{a, c\}$, $A \cap C = \{c\}$, $B \cap C = \{c, g\}$; $A \cap (B \cup C) = \{a, c\}$;
$(A \cap B) \cup C = \{a, c, g, m, n, p\}$, $(A \cup B) \cap C = \{c, g\}$, $(A \cap B) \cup (A \cap C) = A \cap (B \cup C)$.

3. Sean los subconjuntos $K = \{2, 4, 6, 8\}$, $L = \{1, 2, 3, 4\}$, $M = \{3, 4, 5, 6, 8\}$ de $U = \{1, 2, 3, \ldots, 10\}$. (*a*) Poner K', L', M' en forma tabular. (*b*) Mostrar que $(K \cup L)' = K' \cap L'$.

(*a*) $K' = \{1, 3, 5, 7, 9, 10\}$, $L' = \{5, 6, 7, 8, 9, 10\}$, $M' = \{1, 2, 7, 9, 10\}$.
(*b*) $K \cup L = \{1, 2, 3, 4, 6, 8\}$ y así $(K \cup L)' = \{5, 7, 9, 10\}$. Con lo que $K' \cap L' = \{5, 7, 9, 10\} = (K \cup L)'$.

4. Para los conjuntos del Problema 2, mostrar (*a*) $(A \cup B) \cup C = A \cup (B \cup C)$, (*b*) $(A \cap B) \cap C = A \cap (B \cap C)$.

(*a*) Como $A \cup B = \{a, b, c, d, g\}$ y $C = \{c, g, m, n, p\}$, se tiene $(A \cup B) \cup C = \{a, b, c, d, g, m, n, p\}$. Como $A = \{a, b, c, d\}$ y $B \cup C = \{a, c, g, m, n, p\}$, se tiene $A \cup (B \cup C) = \{a, b, c, d, g, m, n, p\} = (A \cup B) \cup C$.
(*b*) Como $A \cap B = \{a, c\}$, se tiene $(A \cap B) \cap C = \{c\}$. Como $B \cap C = \{c, g\}$, se tiene $A \cap (B \cap C) = \{c\} = (A \cap B) \cap C$.

5. En la Fig. 1-1(*c*), sean $C = A \cap B$, $D = A \cap B'$, $E = B \cap A'$ y $F = (A \cup B)'$. Comprobar que:

(*a*) $(A \cup B)' = A' \cap B'$, (*b*) $(A \cap B)' = A' \cup B'$.
(*a*) $A' \cap B' = (E \cup F) \cap (D \cup F) = F = (A \cup B)'$
(*b*) $A' \cup B' = (E \cup F) \cup (D \cup F) = (E \cup F) \cup D = C' = (A \cap B)'$

6. Con el diagrama de Venn de la Fig. 1-7 comprobar que:

(*a*) $E = (A \cap B) \cap C'$
(*b*) $A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C)$
(*c*) $A \cup B \cap C$ es ambiguo
(*d*) $A' \cap C' = G \cup L$

(*a*) $A \cap B = D \cup E$ y $C' = E \cup F \cup G \cup L$; luego
$(A \cap B) \cap C' = E$

(*b*) $A \cup B \cup C = E \cup F \cup G \cup D \cup H \cup J \cup K$. Ahora,
$A \cup B = E \cup F \cup G \cup D \cup H \cup J$
y $C = D \cup H \cup J \cup K$
de modo que
$(A \cup B) \cup C = E \cup F \cup G \cup D \cup H \cup J \cup K$
$= A \cup B \cup C$

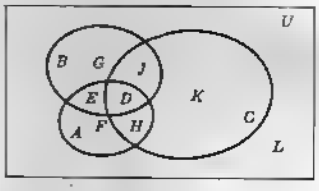


Fig. 1-7

Asimismo, $B \cup C = E \cup G \cup D \cup H \cup J \cup K$ y $A = E \cup F \cup D \cup H$
con lo que $A \cup (B \cup C) = E \cup F \cup G \cup D \cup H \cup J \cup K = A \cup B \cup C$

(*c*) $A \cup B \cap C$ se podría interpretar ya como $(A \cup B) \cap C$ ya como $A \cup (B \cap C)$. Ahora bien, $(A \cup B) \cap C = D \cup H \cup J$, mientras que $A \cup (B \cap C) = A \cup (D \cup J) = A \cup J$. Así, pues, $A \cup B \cap C$ es ambiguo.
(*d*) $A' = G \cup J \cup K \cup L$ y $C' = E \cup F \cup G \cup L$; de donde, $A' \cap C' = G \cup L$.

7. Sean A y B subconjuntos de U. Ilustrar con diagramas de Venn: $A \cap B' = A$ si, y solo si, $A \cap B = \varnothing$.

Supóngase $A \cap B = \varnothing$ con referencia a la Fig. 1-1(*b*). Pero $A \subset B'$; luego $A \cap B' = A$.
Supóngase $A \cap B \neq \varnothing$ con referencia a la Fig. 1-1(*c*). Pero $A \not\subset B'$; luego $A \cap B' \neq A$.
Así, pues, $A \cap B' = A$ si, y solo si, $A \cap B = \varnothing$.

8. Demostrar que $(A \cup B) \cup C = A \cup (B \cup C)$.

Sea $x \in (A \cup B) \cup C$. Entonces $x \in A \cup B$ o bien $x \in C$, de modo que $x \in A$ o bien $x \in B$ o bien $x \in C$. Si $x \in A$, entonces $x \in A \cup (B \cup C)$; si $x \in B$ o bien $x \in C$, entonces $x \in B \cup C$ y, por tanto, $x \in A \cup (B \cup C)$. Así, pues, $(A \cup B) \cup C \subseteq A \cup (B \cup C)$.

Sea $x \in A \cup (B \cup C)$. Entonces $x \in A$ o bien $x \in B \cup C$, con lo que $x \in A$ o $x \in B$ o $x \in C$. Si $x \in A$ o $x \in B$, es $x \in A \cup B$ y entonces $x \in (A \cup B) \cup C$; si $x \in C$, es $x \in (A \cup B) \cup C$. Así que $A \cup (B \cup C) \subseteq (A \cup B) \cup C$.

Pero $(A \cup B) \cup C \subseteq A \cup (B \cup C)$ y $A \cup (B \cup C) \subseteq (A \cup B) \cup C$ implica $(A \cup B) \cup C = A \cup (B \cup C)$ como se afirmaba. Así, pues, $A \cup B \cup C$ es inequívoco.

9. Demostrar: $(A \cap B) \cap C = A \cap (B \cap C)$.

Sea $x \in (A \cap B) \cap C$. Entonces $x \in A \cap B$ y $x \in C$, de modo que $x \in A$ y $x \in B$ y $x \in C$. Como $x \in B$ y $x \in C$, entonces $x \in B \cap C$; como $x \in A$ y $x \in B \cap C$, entonces $x \in A \cap (B \cap C)$. Así, pues, $(A \cap B) \cap C \subseteq A \cap (B \cap C)$.

Sea $x \in A \cap (B \cap C)$. Entonces $x \in A$ y $x \in B \cap C$, con lo que $x \in A$ y $x \in B$ y $x \in C$. Como $x \in A$ y $x \in B$, entonces $x \in A \cap B$; como $x \in A \cap B$ y $x \in C$, entonces $x \in (A \cap B) \cap C$. Así que $A \cap (B \cap C) \subseteq (A \cap B) \cap C$ y $(A \cap B) \cap C = A \cap (B \cap C)$ como se afirmaba. Así, $A \cap B \cap C$ es inequívoco.

10. Demostrar: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Sea $x \in A \cap (B \cup C)$. Entonces $x \in A$ y $x \in B \cup C$ ($x \in B$ o $x \in C$), de modo que $x \in A$ y $x \in B$ o $x \in A$ y $x \in C$. Si $x \in A$ y $x \in B$, entonces $x \in A \cap B$ y así $x \in (A \cap B) \cup (A \cap C)$; de igual modo, si $x \in A$ y $x \in C$, es $x \in A \cap C$ y así $x \in (A \cap B) \cup (A \cap C)$. Con lo que $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

Sea $x \in (A \cap B) \cup (A \cap C)$, con lo que $x \in A \cap B$ o $x \in A \cap C$. Si $x \in A \cap B$, entonces $x \in A$ y $x \in B$ de modo que $x \in A$ y $x \in B \cup C$; análogamente, si $x \in A \cap C$, entonces $x \in A$ y $x \in C$ con lo que $x \in A$ y $x \in B \cup C$. Así, pues, $x \in A \cap (B \cup C)$ y $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Por último, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ según lo afirmado.

11. Demostrar: $(A \cup B)' = A' \cap B'$.

Sea $x \in (A \cup B)'$. Como $x \notin A \cup B$, entonces $x \notin A$ y $x \notin B$. O sea, que $x \in A'$ y $x \in B'$, esto es, $x \in A' \cap B'$; luego $(A \cup B)' \subseteq A' \cap B'$.

Sea $x \in A' \cap B'$. Como $x \in A'$ y $x \in B'$, se tiene $x \notin A$ y $x \notin B$. Entonces $x \notin A \cup B$, de modo que $x \in (A \cup B)'$; luego $A' \cap B' \subseteq (A \cup B)'$. Así que $(A \cup B)' = A' \cap B'$ como se afirmaba.

12. Demostrar: $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

$$C \cup (A \cap B) = (C \cup A) \cap (C \cup B) \qquad \text{por (1.10), página 5.}$$

Y entonces

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C) \qquad \text{por (1.9), página 5.}$$

13. Demostrar: $A - (B \cup C) = (A - B) \cap (A - C)$.

Sea $x \in A - (B \cup C)$. Como $x \in A$ y $x \notin B \cup C$, se tiene, $x \in A$ pero $x \notin B$ y $x \notin C$. Entonces $x \in A - B$ y $x \in A - C$, con lo que $x \in (A - B) \cap (A - C)$ y $A - (B \cup C) \subseteq (A - B) \cap (A - C)$.

Sea $x \in (A - B) \cap (A - C)$. Como $x \in A - B$ y $x \in A - C$, es decir, $x \in A$ pero $x \notin B$ y $x \notin C$. Se tiene $x \in A$ pero $x \notin B \cup C$, así que $x \in A - (B \cup C)$ y $(A - B) \cap (A - C) \subseteq A - (B \cup C)$. De modo que $A - (B \cup C) = (A - B) \cap (A - C)$ según lo afirmado.

14. Demostrar: $(A \cup B) \cap B' = A$ si, y solo si, $A \cap B = \varnothing$.

Mediante (1.10') y (1.7'), página 5, hallamos que

$$(A \cup B) \cap B' = (A \cap B') \cup (B \cap B') = A \cap B'$$

Hay que demostrar, pues, que: $A \cap B' = A$ si, y solo si, $A \cap B = \varnothing$.

(*a*) Supuesto $A \cap B = \varnothing$, es $A \subseteq B'$ y $A \cap B' = A$.

(*b*) Supuesto $A \cap B' = A$, es $A \subseteq B'$ y $A \cap B = \varnothing$.

Así que $(A \cup B) \cap B' = A$ si (por (*a*)) y solo si (por (*b*)) $A \cap B = \varnothing$.

15. Demostrar: $X \subseteq Y$ si, y solo si, $Y' \subseteq X'$.

(i) Supóngase $X \subseteq Y$. Sea $y' \in Y'$. Entonces $y' \notin X$ como $y' \notin Y$; de donde $y' \in X'$ y $Y' \subseteq X'$.
(ii) Recíprocamente, supóngase $Y' \subseteq X'$. Ahora, por (i), $(X')' \subseteq (Y')'$; de donde $X \subseteq Y$.

16. Demostrar la identidad $(A - B) \cup (B - A) = (A \cup B) - (A \cap B)$ del Ejemplo 10 usando la identidad $A - B = A \cap B'$ del Ejemplo 9.

Tenemos

$$\begin{aligned}
(A - B) \cup (B - A) &= (A \cap B') \cup (B \cap A') && \text{por (1.10), página 5} \\
&= [(A \cap B') \cup B] \cap [(A \cap B') \cup A'] && \text{por (1.10)} \\
&= [(A \cup B) \cap (B' \cup B)] \cap [(A \cup A') \cap (B' \cup A')] && \text{por (1.7)} \\
&= [(A \cup B) \cap U] \cap [U \cap (B' \cup A')] && \text{por (1.4')} \\
&= (A \cup B) \cap (B' \cup A') && \text{por (1.9)} \\
&= (A \cup B) \cap (A' \cup B') && \text{por (1.11')} \\
&= (A \cup B) \cap (A \cap B)' \\
&= (A \cup B) - (A \cap B)
\end{aligned}$$

17. Demostrar que dos segmentos cualesquiera tienen tantos puntos el uno como el otro.

Sean los segmentos AB y $A'B'$ de la Fig. 1-8. Vamos a demostrar que siempre es posible una biyección entre ambos. Llamando P la intersección de AB' y BA', dado cualquier punto C de AB sea C' la intersección de CP con $A'B'$. La aplicación

$$C \to C'$$

es la biyección buscada, pues cada punto de AB tiene una imagen única en $A'B'$ y cada punto $A'B'$ es la imagen de un único punto de AB.

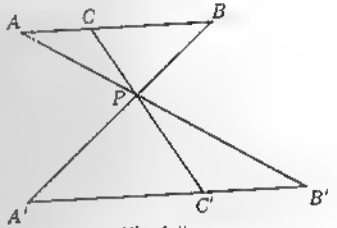


Fig. 1-8

18. Demostrar: (*a*) $x \to x + 2$ es inyección, pero no sobreyección, de N en N. (*b*) $x \to 3x - 2$ es biyección de Q sobre Q. (*c*) $x \to x^3 - 3x^2 - x$ es sobreyección de R en R pero no inyección.

(*a*) Está claro que $x + 2 \in N$ si $x \in N$. La aplicación no es sobreyectiva puesto que 2 no es imagen.

(*b*) Evidentemente, $3x - 2 \in Q$ si $x \in Q$. Y también todo $r \in Q$ es imagen de $x = (r + 2)/3 \in Q$.

(*c*) Claro es que $x^3 - 3x^2 - x \in R$ si $x \in R$. Así que si $r \in R$, $x^3 - 3x^2 - x = r$ tiene siempre una raíz real x cuya imagen es r. Si $r = -3$, $x^3 - 3x^2 - x = r$ tiene 3 raíces reales $x = -1, 1, 3$. Como cada una de éstas tiene $r = -3$ por imagen, la aplicación no es inyectiva.

19. Demostrar: Si α es biyección entre S y T, α tiene una recíproca única y al contrario.

Supóngase que α es una aplicación biyectiva de S sobre T; entonces, para cualquier $s \in S$, se tiene

$$s \to s\alpha = t \in T$$

Siendo t único, se sigue que α induce una aplicación inyectiva

$$\beta: \quad t\beta \to s$$

Ahora bien, $s(\alpha\beta) = (s\alpha)\beta = t\beta = s$; luego $\alpha\beta = \mathscr{I}$ y β es una recíproca de α. Suponiendo que esta recíproca no es única, sea γ otra recíproca de α. Puesto que

$$\alpha\beta = \beta\alpha = \mathscr{I} \qquad \text{y} \qquad \alpha\gamma = \gamma\alpha = \mathscr{I}$$

se sigue que

$$\beta\alpha\gamma = \beta(\alpha\gamma) = \beta \cdot \mathcal{J} = \beta$$

y

$$\beta\alpha\gamma = (\beta\alpha)\gamma = \mathcal{J} \cdot \gamma = \gamma$$

Así, pues, $\beta = \gamma$: la recíproca de α es única.

Y al contrario, sea α^{-1} la recíproca única de la aplicación α de S en T. Supóngase que para $s_1, s_2 \in S$, con $s_1 \neq s_2$ se tenga $s_1\alpha = s_2\alpha$. Entonces $(s_1\alpha)\alpha^{-1} = (s_2\alpha)\alpha^{-1}$, de modo que $s_1(\alpha \cdot \alpha^{-1}) = s_2(\alpha \cdot \alpha^{-1})$ y $s_1 = s_2$ en contradicción con lo supuesto. Así, pues, α es una aplicación inyectiva. Y como para todo $t \in T$, se tiene $(t\alpha^{-1})\alpha = t(\alpha^{-1} \cdot \alpha) = t \cdot \mathcal{I} = t$, es t la imagen de $s = t\alpha^{-1} \in S$ y la aplicación es sobreyectiva.

20. Demostrar: Si α es una biyección entre S y T y β es biyección entre T y U, entonces $(\alpha\beta)^{-1} = \beta^{-1} \cdot \alpha^{-1}$.

Como $(\alpha\beta)(\beta^{-1} \cdot \alpha^{-1}) = \alpha(\beta \cdot \beta^{-1})\alpha^{-1} = \alpha \cdot \alpha^{-1} = \mathcal{I}$, $\beta^{-1} \cdot \alpha^{-1}$ es una recíproca de $\alpha\beta$; y por el Problema 19 una recíproca semejante es única; luego $(\alpha\beta)^{-1} = \beta^{-1} \cdot \alpha^{-1}$.

$A \cup B \supset B \cup A$
$(A \cup B) \cap C$

Problemas propuestos

21. Indicar en forma tabular:

(*a*) el conjunto de los enteros negativos mayores que -6,

(*b*) el conjunto de los enteros entre -3 y 4,

(*c*) el conjunto de los enteros cuyos cuadrados son menores que 20,

(*d*) el conjunto de todos los factores positivos de 18,

(*e*) el conjunto de todos los factores positivos comunes de 16 y 24,

(*f*) $\{p:\ p \in N,\ p^2 < 10\}$

(*g*) $\{b:\ b \in N,\ 3 \leq b \leq 8\}$

(*h*) $\{x:\ x \in I,\ 3x^2 + 7x + 2 = 0\}$

(*i*) $\{x:\ x \in Q,\ 2x^2 + 5x + 3 = 0\}$

Respuesta parcial: (*a*) $\{-5, -4, -3, -2, -1\}$, (*d*) $\{1, 2, 3, 6, 9, 18\}$, (*f*) $\{1, 2, 3\}$, (*h*) $\{-2\}$

22. Comprobar: (*a*) $\{x:\ x \in N,\ x < 1\} = \varnothing$, (*b*) $\{x:\ x \in Z,\ 6x^2 + 5x - 4 = 0\} = \varnothing$.

23. Dar los 15 subconjuntos propios de $S = \{a, b, c, d\}$.

24. Demostrar que los subconjuntos propios de $S = \{a_1, a_2, \ldots, a_n\}$ son $2^n - 1$ en número.

25. Con los conjuntos del Problema 2, comprobar:
(*a*) $(A \cup B) \cup C = A \cup (B \cup C)$. (*b*) $(A \cap B) \cap C = A \cap (B \cap C)$. (*c*) $(A \cup B) \cap C \neq A \cup (B \cap C)$.

26. Con los conjuntos del Problema 3, comprobar: (*a*) $(K')' = K$, (*b*) $(K \cap L)' = K' \cup L'$, (*c*) $(K' \cup L \cup M)' = K' \cap L' \cap M'$, (*d*) $K \cap (L \cup M) = (K \cap L) \cup (K \cap M)$.

27. Si «$n|m$» significa «n es factor de m», dados $A = \{x:\ x \in N,\ 3|x\}$ y $B = \{x:\ x \in N,\ 5|x\}$ enumerar los 4 elementos de cada uno de los conjuntos A', B', $A \cup B$, $A \cap B$, $A \cup B'$, $A \cap B'$, $A' \cup B'$, donde A' y B' son los complementos respectivos de A y B en N.

28. Demostrar las leyes de (1.8)-(1.12'), página 5, que no se han tratado en los Problemas 8-13.

29. Sean A y B subconjuntos de un conjunto universal U. Demostrar:
(*a*) $A \cup B = A \cap B$ si, y solo si, $A = B$.
(*b*) $A \cap B = A$ si, y solo si, $A \subseteq B$.
(*c*) $(A \cap B') \cup (A' \cap B) = A \cup B$ si, y solo si, $A \cap B = \emptyset$.

30. Dados $n(U) = 692$, $n(A) = 300$, $n(B) = 230$, $n(C) = 370$, $n(A \cap B) = 150$, $n(A \cap C) = 180$, $n(B \cap C) = 90$, $n(A \cap B' \cap C') = 10$ siendo $n(S)$ el número de elementos distintos del conjunto S, hallar:
(*a*) $n(A \cap B \cap C) = 40$ (*c*) $n(A' \cap B' \cap C') = 172$
(*b*) $n(A' \cap B \cap C') = 30$ (*d*) $n((A \cap B) \cup (A \cap C) \cup (B \cap C)) = 340$

31. Dadas las aplicaciones α: $n \to n^2 + 1$ y β: $n \to 3n + 2$ de N en N, hallar: $\alpha\alpha = n^4 + 2n^2 + 2$, $\beta\beta$, $\alpha\beta = 3n^2 + 5$, y $\beta\alpha$.

32. ¿Cuáles de las siguientes aplicaciones de Z en Z:

(*a*) $x \to x + 2$, (*b*) $x \to 3x$, (*c*) $x \to x^2$, (*d*) $x \to 4 - x$, (*e*) $x \to x^3$, (*f*) $x \to x^2 - x$

son (i) aplicaciones de Z sobre Z, (ii) biyecciones de Z sobre Z? *Resp.* (i), (ii): (*a*), (*d*)

33. Igual que el Problema 32 con Q en vez de Z. *Resp.* (i), (ii): (*a*), (*b*), (*d*)

34. Igual que el Problema 32 con R en vez de Z. *Resp.* (i), (ii): (*a*), (*b*), (*d*), (*e*)

35. (*a*) Si E es el conjunto de todos los enteros pares positivos, demostrar que $x \to x + 1$, $x \in E$ no es una aplicación sobreyectiva de E en el conjunto F de todos los positivos impares.
(*b*) Si E^* es el conjunto que consiste en el cero y todos los enteros positivos pares (o sea los enteros no negativos), demostrar que $x \to x + 1$, $x \in E^*$ es una sobreyección de E^* en F.

36. Dadas las aplicaciones sobreyectivas

$$\begin{aligned}
\mathcal{J}: &\quad 1\mathcal{J} = 1,\ 2\mathcal{J} = 2,\ 3\mathcal{J} = 3,\ 4\mathcal{J} = 4\\
\alpha: &\quad 1\alpha = 2,\ 2\alpha = 3,\ 3\alpha = 4,\ 4\alpha = 1\\
\beta: &\quad 1\beta = 4,\ 2\beta = 1,\ 3\beta = 2,\ 4\beta = 3\\
\gamma: &\quad 1\gamma = 3,\ 2\gamma = 4,\ 3\gamma = 1,\ 4\gamma = 2\\
\delta: &\quad 1\delta = 1,\ 2\delta = 4,\ 3\delta = 3,\ 4\delta = 2
\end{aligned}$$

de $S = \{1, 2, 3, 4\}$ sobre sí mismo, comprobar:

(*a*) $\alpha\beta = \beta\alpha = \mathcal{J}$, luego $\beta = \alpha^{-1}$; (*b*) $\alpha\gamma = \gamma\alpha = \beta$; (*c*) $\alpha\delta \neq \delta\alpha$; (*d*) $\alpha^2 = \alpha\alpha = \gamma$; (*e*) $\gamma^2 = \mathcal{J}$, luego $\gamma^{-1} = \gamma$; (*f*) $\alpha^4 = \mathcal{J}$, luego $\alpha^3 = \alpha^{-1}$; (*g*) $(\alpha^2)^{-1} = (\alpha^{-1})^2$.

Capítulo 2

Relaciones y operaciones

RELACIONES

Sea el conjunto $P = \{a, b, c, \ldots, t\}$ de todas las personas que viven en una determinada manzana que da a la calle Mayor. Trataremos en esta sección de enunciados, tales como «a es hermano de p», «c es el padre de g», . . . , que se llaman relaciones sobre (o en) el conjunto P. Análogamente, «es paralela a», «es perpendicular a», «forma un ángulo de 45° con», . . . , son relaciones en el conjunto L de todas las rectas de un plano.

Supóngase en el conjunto P anterior que los únicos padres son c, d, g y que

c es el padre de a, g, m, p, q
d es el padre de f
g es el padre de h, n

Entonces, haciendo que $\mathscr{R}$ signifique «es el padre de», podemos escribir

$$c \mathscr{R} a,\ c \mathscr{R} g,\ c \mathscr{R} m,\ c \mathscr{R} p,\ c \mathscr{R} q,\ d \mathscr{R} f,\ g \mathscr{R} h,\ g \mathscr{R} n$$

Pero $c \mathscr{R} a$ puede mirarse como la determinación de un par ordenado, bien sea (a, c) o bien (c, a), del conjunto producto $P \times P$. Si bien se emplean ambas maneras, aquí *siempre* asociaremos

$$c \mathscr{R} a \text{ con el par ordenado } (a, c)$$

Esto supuesto, $\mathscr{R}$ determina en P el conjunto de pares ordenados

$$(a, c),\ (g, c),\ (m, c),\ (p, c),\ (q, c),\ (f, d),\ (h, g),\ (n, g)$$

Así como ocurrió con el término función en el Capítulo 1, definimos la relación $\mathscr{R}$ diciendo que es este subconjunto de $P \times P$. Así, pues,

Una *relación* $\mathscr{R}$ sobre un conjunto S (con más precisión, una *relación binaria* sobre S, pues es una relación entre pares de elementos de S) es un subconjunto de $S \times S$.

Ejemplo 1:

(*a*) Sea $S = \{2, 3, 5, 6\}$ y dése a $\mathscr{R}$ el significado «divide a».
Como $2 \mathscr{R} 2,\ 2 \mathscr{R} 6,\ 3 \mathscr{R} 3,\ 3 \mathscr{R} 6,\ 5 \mathscr{R} 5,\ 6 \mathscr{R} 6$, se tiene
$$\mathscr{R} = \{(2, 2),\ (6, 2),\ (3, 3),\ (6, 3),\ (5, 5),\ (6, 6)\}$$

(*b*) Sea $S = \{1, 2, 3, \ldots, 20\}$ y $\mathscr{R}$ signifique «es triple de».
Entonces $3 \mathscr{R} 1,\ 6 \mathscr{R} 2,\ 9 \mathscr{R} 3,\ 12 \mathscr{R} 4,\ 15 \mathscr{R} 5,\ 18 \mathscr{R} 6$ y
$$\mathscr{R} = \{(1, 3),\ (2, 6),\ (3, 9),\ (4, 12),\ (5, 15),\ (6, 18)\}$$

(*c*) Examínese ahora $\mathscr{R} = \{(x, y) : 2x - y = 6,\ x \in \mathscr{R}\}$. Geométricamente, cada $(x, y) \in \mathscr{R}$ es un punto del grafo de la ecuación $2x - y = 6$. Así, pues, si pudo parecer extraño antes decir que

$$c \mathscr{R} a \text{ significa } (a, c) \in \mathscr{R} \text{ y no } (c, a) \in \mathscr{R}$$

ahora ya se ve que esto concuerda con la idea de que toda ecuación $y = f(x)$ no es más que una relación binaria especial.

PROPIEDADES DE LAS RELACIONES BINARIAS

Se dice que una relación $\mathscr{R}$ sobre un conjunto S es *reflexiva* si $a \mathscr{R} a$ para todo $a \in S$.

Ejemplo 2: (*a*) Sea T el conjunto de todos los triángulos de un plano y dése a $\mathscr{R}$ el significado «es congruente con». Como todo triángulo $t \in T$ es congruente consigo mismo, $t \mathscr{R} t$ para todo $t \in T$, y $\mathscr{R}$ es reflexiva.

(*b*) Para el conjunto T sea $\mathscr{R}$ «tiene doble área que». Es claro que $t \mathscr{R} t$ y $\mathscr{R}$ no es reflexiva.

Una relación $\mathscr{R}$ sobre un conjunto S se dice *simétrica* si cuando $a \mathscr{R} b$ también $b \mathscr{R} a$

Ejemplo 3: (*a*) Sea P el conjunto de personas que habitan en una manzana sobre la calle Mayor, y sea $\mathscr{R}$ «tiene el mismo nombre que». Si x tiene el mismo nombre que y, y tiene el mismo nombre que x; así que $x \mathscr{R} y$ implica $y \mathscr{R} x$ y $\mathscr{R}$ es simétrica.

(*b*) Para el mismo conjunto P, sea la $\mathscr{R}$ «es hermano de». Con $x \mathscr{R} y$, y puede ser hermano o hermana de x; así que $x \mathscr{R} y$ no implica necesariamente $y \mathscr{R} x$ y $\mathscr{R}$ no es simétrica.

Una relación $\mathscr{R}$ sobre un conjunto S se dice *transitiva* si de $a \mathscr{R} b$ y $b \mathscr{R} c$ se sigue $a \mathscr{R} c$.

Ejemplo 4: (*a*) Sea S el conjunto de todas las rectas de un plano y sea $\mathscr{R}$ «es paralela a». Es claro que si a es paralela a b y si b es paralela a otra recta c, entonces a es paralela a c y $\mathscr{R}$ es transitiva.

(*b*) Para el mismo conjunto, S, sea $\mathscr{R}$ «es perpendicular a». Como de a perpendicular a b y de b perpendicular a c resulta a paralela a c, esta $\mathscr{R}$ no es transitiva.

RELACIONES DE EQUIVALENCIA

Una relación $\mathscr{R}$ sobre un conjunto S se llama *relación de equivalencia* sobre S si $\mathscr{R}$ es (i) reflexiva, (ii) simétrica, y (iii) transitiva.

Ejemplo 5: La relación «=» sobre el conjunto R es indudablemente la relación de equivalencia más familiar.

Ejemplo 6: ¿La relación «tiene el mismo nombre que» sobre el conjunto P del Ejemplo 3 es una relación de equivalencia?

Habrá que verificar la validez de lo que se establece en seguida entre elementos arbitrarios $x, y, z \in P$:

(i) x tiene el mismo nombre que x.

(ii) Si x tiene el mismo nombre que y, entonces y tiene el mismo nombre que x.

(iii) Si x tiene el mismo nombre que y y si y tiene el mismo nombre que z, entonces x tiene el mismo nombre que z.

Como todo esto es cierto, «tiene el mismo nombre que» es (i) reflexiva, (ii) simétrica, (iii) transitiva y, por tanto, se trata de una relación de equivalencia sobre P.

Ejemplo 7: Se sigue del Ejemplo 3(*b*) que «es hermano de» no es simétrica y que, por tanto, no es una relación de equivalencia sobre P.

Véanse Problemas 1-3.

CLASES DE EQUIVALENCIA

Sean un conjunto S y una relación $\mathscr{R}$ de equivalencia sobre S. Si $a \in S$, los elementos $y \in S$ que verifican $y \mathscr{R} a$ constituyen un subconjunto, $[a]$, de S, llamado *clase de equivalencia*. Así, pues,

$$[a] = \{y;\ y \in S,\ y \mathscr{R} a\}$$

(Obsérvese el empleo de corchetes para indicar clases de equivalencia.)

Ejemplo 8: Considérese el conjunto T de los triángulos de un plano y la relación de equivalencia (véase Problema 1) «es congruente con». Siendo $a, b \in T$ entenderemos por $[a]$ el conjunto o clase de equivalencia de todos los triángulos de T congruentes con el triángulo a, y por $[b]$ el conjunto o clase de todos los triángulos congruentes con el triángulo b. Notemos de paso que el triángulo a está incluido en $[a]$ y que si un triángulo c está tanto en $[a]$ como en $[b]$, entonces $[a]$ y $[b]$ no son más que otras dos maneras de denotar la clase $[c]$.

Un conjunto $\{A, B, C, \ldots\}$ de subconjuntos no vacíos de un conjunto S se llama *partición* de S si (i) $A \cup B \cup C \cup \cdots = S$ y si (ii) la intersección de cada dos subconjuntos distintos es vacía. El resultado principal de esta sección es el

Teorema I. Una relación de equivalencia $\mathscr{R}$ sobre un conjunto S produce una partición de S y, recíprocamente, una partición de S define una relación de equivalencia sobre S.

Ejemplo 9: Se dice que dos enteros tienen la misma paridad si ambos son pares o si ambos son impares. La relación «tiene la misma paridad que» sobre Z es una relación de equivalencia. (Demuéstrese.) La relación da lugar a dos subconjuntos de Z:

$$A = \{x: x \in Z,\ x \text{ es par}\} \quad \text{y} \quad B = \{x: x \in Z,\ x \text{ es impar}\}$$

Y todo elemento de Z se encontrará ya en A ya en B, pero no en ambos. Así, pues, $A \cup B = Z$ y $A \cap B = \varnothing$, de modo que la relación efectúa una partición de Z.

Ejemplo 10: Y todo elemento de Z se encontrará ya en A ya en B, pero no en ambos. Así, pues, $A \cup B = Z$ del $S = \{1, 2, 3, \ldots, 25\}$. Es evidente que $A \cup B \cup C = S$ y que $A \cap B = A \cap C = B \cap C = \varnothing$, así que $\{A, B, C\}$ es una partición de S. La relación de equivalencia que da lugar a esta partición es «da el mismo resto dividido por 3 que».

Para demostrar el Teorema I (véase Problema 6), se utilizarán las propiedades que siguen de las clases de equivalencia:

(1) $a \in [a]$

(2) Si $b \in [a]$, es $[b] = [a]$.

(3) Si $[a] \cap [b] \neq \varnothing$, es $[a] = [b]$.

La primera resulta inmediatamente de la propiedad reflexiva $a \mathscr{R} a$ de una relación de equivalencia. Para las otras, véanse Problemas 4-5.

ORDEN EN UN CONJUNTO

Sea el subconjunto $A = \{2, 1, 3, 12, 4\}$ de N. Al escribirlo se ha evitado exprofeso seguir la natural inclinación de enunciarlo como $A = \{1, 2, 3, 4, 12\}$ para indicar que esta última versión resulta de valerse de la relación binaria $(\leq)$ definida sobre N. Esta ordenación de los elementos de A (o sea, de N) se dice *total*, ya que para todo $a, b \in A$ $(m, n \in N)$ se tiene o bien $a < b$, o bien $a = b$, o bien $a > b$ $(m < n, m = n, m > n)$. Por otra parte, la relación binaria $(|)$, (véase Problema 27, Capítulo 1) produce solamente una *ordenación parcial* de A, es decir $2 | 4$ pero $2 \nmid 3$. Estas ordenaciones de A se pueden ilustrar del mejor modo con diagramas. La Fig. 2-1 muestra la ordenación de A efectuada por $(\leq)$. Se comienza en el punto más bajo del diagrama y se siguen las flechas para obtener

$$1 \leq 2 \leq 3 \leq 4 \leq 12$$

Fig. 2-1

Fig. 2-2

Es de esperar que el diagrama de un conjunto totalmente ordenado sea siempre una línea recta. La Figura 2-2 ilustra el orden parcial de A efectuado por la relación $(|)$.

Véase también Problema 7.

Un conjunto S se dice *parcialmente ordenado* (no se excluye la posibilidad del orden total) por una relación binaria $\mathscr{R}$ si para cualesquiera $a, b, c \in S$,

(i) $\mathscr{R}$ es reflexiva, esto es, $a \mathscr{R} a$

(ii') $\mathscr{R}$ es antisimétrica, es decir, $a \mathscr{R} b$ y $b \mathscr{R} a$ si, y solo si, $a = b$

(iii) $\mathscr{R}$ es transitiva, es decir, $a \mathscr{R} b$ y $b \mathscr{R} c$ implican $a \mathscr{R} c$

Se deja al cuidado del lector verificar que estas propiedades las cumplen las relaciones ($\preceq$) y ($|$) sobre A y que las propiedades contienen una redundancia porque (ii') implica (i). La redundancia se ha introducido para que se vea perfectamente clara la diferencia esencial entre las relaciones de esta sección y las de la precedente.

Sea S un conjunto parcialmente ordenado con respecto a $\mathscr{R}$. Entonces:

(1) Todo subconjunto de S está también parcialmente ordenado con respecto a $\mathscr{R}$ a la vez que algunos subconjuntos pueden estar totalmente ordenados. Por ejemplo, en la Fig. 2-2, el subconjunto $\{1, 2, 3\}$ está parcialmente ordenado, en tanto que el subconjunto $\{1, 2, 4\}$ está totalmente ordenado por la relación ($|$).

(2) El elemento $a \in S$ se dice un *primer elemento* de S si $a \mathscr{R} x$ para todo $x \in S$.

(3) El elemento $g \in S$ se dice un *último elemento* de S si $x \mathscr{R} g$ para todo $x \in S$.

[El primero (último) elemento de un conjunto ordenado, si existe, es único.]

(4) El elemento $a \in S$ se dice un *elemento minimal* de S si $x \mathscr{R} a$ implica $x = a$ para todo $x \in S$.

(5) El elemento $g \in S$ se dice un *elemento maximal* de S si $g \mathscr{R} x$ implica $g = x$ para todo $x \in S$.

Ejemplo 11: (*a*) En las ordenaciones de A de las Figs. 2-1 y 2-2, el primer elemento es 1 y el último elemento es 12. Asimismo, 1 es un elemento minimal y 12 es un elemento maximal.

(*b*) En la Fig. 2-3, $S = \{a, b, c, d\}$ tiene un primer elemento a, pero no tiene último. Aquí a es un elemento minimal, en tanto que c y d son elementos maximales.

(*c*) En la Fig. 2-4, $S = \{a, b, c, d, e\}$ tiene un último elemento e, pero carece de primer elemento. Aquí a y b son elementos minimales, mientras que e es un elemento maximal.

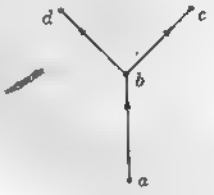


Fig. 2-3

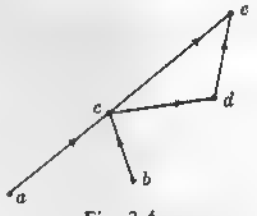


Fig. 2-4

Si un conjunto ordenado S tiene la propiedad de que cada uno de sus subconjuntos no vacíos tiene primer elemento, se dice que está *bien ordenado*. Por ejemplo, considérense los conjuntos N y Q ordenado cada uno por la relación ($\leq$). Se ve que N es bien ordenado; pero, dado que el subconjunto $\{x: x \in Q, x > 2\}$ de Q no tiene primer elemento, Q no es bien ordenado en cambio. ¿Está Z bien ordenado por la relación ($\leq$)? ¿Está $A = \{1, 2, 3, 4, 12\}$ bien ordenado por la relación ($|$)?

Sea S un conjunto bien ordenado por la relación $\mathscr{R}$. Entonces, para cualesquiera $a, b \in S$, el subconjunto $\{a, b\}$ de S tiene primer elemento y, entonces, o bien $a \mathscr{R} b$ o bien $b \mathscr{R} a$. Queda demostrado el

Teorema II. Todo conjunto bien ordenado es totalmente ordenado.

OPERACIONES

Sea $Q^+ = \{x: x \in Q, x > 0\}$. Para cualesquiera $a, b \in Q^+$, se tiene

$$a + b,\ b + a,\ a \cdot b,\ b \cdot a,\ a : b,\ b : a \in Q^+$$

Adición, multiplicación y división son ejemplos de *operaciones binarias* en Q^+. (Obsérvese que semejantes operaciones son simplemente aplicaciones de $Q^+ \times Q^+$ en Q^+.) Por ejemplo, la adición asocia a cada par $a, b \in Q^+$ un elemento $a + b \in Q^+$. Aquí es $a + b = b + a$, pero, en general, $a : b \neq b : a$; de manera que para tener la seguridad de una imagen única, es necesario considerar estas operaciones como definidas para un par ordenado de elementos. Así, pues,

Una *operación binaria* «$\circ$» en un conjunto no vacío S es una aplicación que asocia a cada par ordenado (a, b) de elementos de S un elemento definido único $a \circ b$ de S. Dicho brevemente, una operación binaria en un conjunto S es una aplicación de $S \times S$ en S.

Ejemplo 12: (*a*) La adición es una operación binaria en el conjunto de los números naturales pares (la suma de dos números naturales pares es un número natural par), pero no es una operación binaria en el conjunto de los números naturales impares (la suma de dos números naturales impares es un número natural par).

(*b*) Ni la adición ni la multiplicación son operaciones binarias en $S = \{0, 1, 2, 3, 4\}$, pues, por ejemplo, $2 + 3 = 5 \notin S$ y $2 \cdot 3 = 6 \notin S$.

$\circ$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	(c)
e	e	a	b	c	d

Tabla 2-1

(*c*) La Tabla 2-1 adjunta, que define una cierta operación binaria $\circ$ sobre el conjunto $A = \{a, b, c, d, e\}$ ha de leer así: Para cada par ordenado (x, y) de $A \times A$ se encuentra $x \circ y$ en el cruce de la fila encabezada x y la columna encabezada y. Por ejemplo, el elemento marcado con un círculo es $d \circ e$ (no $e \circ d$).

El hecho de que $\circ$ sea una operación binaria sobre un conjunto S se suele indicar por el enunciado equivalente: El conjunto S es *cerrado* con respecto a la operación $\circ$. El Ejemplo 12(*a*) se puede expresar entonces así: El conjunto de los números naturales pares es cerrado con respecto a la adición; el conjunto de los números naturales impares no es cerrado con respecto a la adición.

PROPIEDADES DE LAS OPERACIONES BINARIAS

Una operación binaria $\circ$ sobre un conjunto S se dice *conmutativa* si $x \circ y = y \circ x$ para todo $x, y \in S$.

Ejemplo 13: (*a*) La adición y la multiplicación son operaciones binarias conmutativas en tanto que la división no es una operación binaria conmutativa sobre Q^+.

(*b*) La operación $\circ$ sobre A de la Tabla 2-1 es conmutativa. Esto se verifica fácilmente notando que (i) cada fila (b, c, d, e, a en la segunda fila, por ejemplo) y la columna con igual encabezamiento (b, c, d, e, a, en la segunda columna) se leen exactamente lo mismo; o bien porque (ii) los elementos de S están situados simétricamente con respecto a la diagonal principal (línea de trazos) que va de la izquierda superior a la derecha inferior de la tabla.

Una operación binaria $\circ$ sobre un conjunto S se dice *asociativa* si $(x \circ y) \circ z = x \circ (y \circ z)$ para cualesquiera $x, y, z \in S$.

Ejemplo 14: (*a*) La adición y la multiplicación son operaciones binarias asociativas sobre Q^+.

(*b*) La operación $\circ$ sobre A de la Tabla 2-1 es asociativa. Se encuentra, por ejemplo, que $(b \circ c) \circ d = d \circ d = b$ y que $b \circ (c \circ d) = b \circ a = b$; $(d \circ e) \circ d = c \circ d = a$ y $d \circ (e \circ d) = d \circ c = a$; . . . . La prueba completa sería en extremo tediosa, pero se sugiere al lector que haga otras cuantas verificaciones al azar.

(*c*) Sea $*$ una operación binaria sobre R, definida por

$$a * b = a + 2b \quad \text{para cualesquiera} \quad a, b \in R$$

Como $(a * b) * c = (a + 2b) * c = a + 2b + 2c$

pero $a * (b * c) = a * (b + 2c) = a + 2(b + 2c) = a + 2b + 4c$

la operación no es asociativa.

Un conjunto S está dotado de elemento *neutro* (*identidad* o *unidad*, también se dice) con respecto a una operación binaria $\circ$ sobre S si existe un elemento $u \in S$ con la propiedad de que $u \circ x = x \circ u = x$ para todo $x \in S$.

Ejemplo 15: (*a*) Un elemento neutro de Q con respecto a la adición es 0 porque $0 + x = x + 0 = x$ para todo $x \in Q$; un elemento neutro de Q con respecto a la multiplicación es 1, puesto que $1 \cdot x = x \cdot 1 = x$ para todo $x \in Q$.

(*b*) N no tiene elemento neutro con respecto a la adición, pero 1 es un elemento neutro respecto de la multiplicación.

(*c*) Un elemento neutro del conjunto A del Ejemplo 12(*c*) con respecto a $\circ$ es a. Nótese que hay solamente uno.

En el Problema 8 demostramos el

Teorema III. El elemento neutro, si existe, de un conjunto S con respecto a una operación binaria $\circ$ sobre S es único.

Sea un conjunto S que posee el elemento neutro u con respecto a una operación binaria $\circ$. Un elemento $y \in S$ se dice *simétrico* de $x \in S$ si $x \circ y = y \circ x = u$.

Ejemplo 16: (*a*) El simétrico con respecto a la adición, o sea el *simétrico aditivo* de $x \in Z$ es $-x$ porque $x + (-x) = 0$, que es el elemento neutro aditivo de Z. El simétrico aditivo se suele llamar opuesto. En general, $x \in Z$ no tiene simétrico multiplicativo.

(*b*) En el Ejemplo 12(*c*), los simétricos de a, b, c, d, e son, respectivamente, a, e, d, c, b.

No es difícil demostrar el

Teorema IV. Sea $\circ$ una operación binaria sobre un conjunto S. El simétrico con respecto a $\circ$ del $x \in S$, si existe, es único.

Por último, sea S un conjunto con dos operaciones binarias $\square$ y $\circ$ definidas sobre él. La operación $\square$ se dice *distributiva a la izquierda* con respecto a $\circ$ si

$$a \square (b \circ c) = (a \square b) \circ (a \square c) \quad \text{para cualesquiera } a, b, c \in S \tag{a}$$

y se dice *distributiva a la derecha* con respecto a $\circ$ si

$$(b \circ c) \square a = (b \square a) \circ (c \square a) \quad \text{para cualesquiera } a, b, c \in S \tag{b}$$

Si se verifican tanto (*a*) como (*b*), se dice simplemente que $\square$ es *distributiva* con respecto a $\circ$. Nótese que los segundos miembros de (*a*) y (*b*) son iguales si $\square$ es conmutativa.

Ejemplo 17: (*a*) En el conjunto de los enteros, la multiplicación ($\square = \cdot$) es distributiva con respecto a la adición ($\circ = +$), ya que $x \cdot (y + Z) = x \cdot y + x \cdot Z$ para todo x, y, $z \in Z$.

(*b*) En el conjunto de los enteros, sea $\circ$ la adición ordinaria y $\square$ la operación definida por

$$x \square y = x^2 \cdot y = x^2 y \quad \text{para cualesquiera} \quad x, y \in Z$$

Como $$a \square (b + c) = a^2 b + a^2 c = (a \square b) + (a \square c)$$

$\square$ es distributiva a la izquierda con respecto a $+$. Como

$$(b + c) \square a = ab^2 + 2abc + ac^2 \neq (b \square a) + (c \square a) = b^2 a + c^2 a$$

$\square$ no es distributiva a la derecha respecto de $+$.

RELACION DE EQUIVALENCIA COMPATIBLE CON UNA OPERACION

Sea $S = \{a, b, c, \ldots\}$ un conjunto en el cual se ha definido una operación $\circ$ y sea una relación de equivalencia $\mathscr{R}$ que produce en S la partición en el conjunto de clases de equivalencia $E = \{[a], [b], [c], \ldots\}$. Si se define sobre E una operación binaria $\oplus$ por

$$[a] \oplus [b] = [a \circ b] \quad \text{para cualesquiera} \quad [a], [b] \in E$$

No se ve de inmediato que para cualesquiera $p, q \in [a]$ y para cualesquiera $r, s \in [b]$, se tenga

$$[p \circ r] = [q \circ s] = [a \circ b] \tag{c}$$

Se dirá que la relación de equivalencia $\mathscr{R}$ es *compatible* con la operación binaria $\oplus$ y que entonces la operación $\oplus$ está *bien definida* si se verifica (*c*), es decir, que

$$[p] \oplus [r] = [q] \oplus [s] = [a] \oplus [b]$$

siempre que (*c*) se verifique y solo entonces.

Ejemplo 18: La relación «da el mismo resto cuando se divide por 9 que» reparte N en nueve clases de equivalencia $[1], [2], [3], \ldots, [9]$. Si $\circ$ se interpreta como adición en N es fácil ver que $\oplus$ queda bien definida de acuerdo con lo dicho arriba. Por ejemplo, si $x, y \in N$, $9x + 2 \in [2]$ y $9y + 5 \in [5]$ entonces $[2] \oplus [5] = [(9x + 2) + (9y + 5)] = [9(x + y) + 7] = [7] = [2 + 5]$, etc.

ISOMORFISMOS

En toda esta sección utilizaremos los dos conjuntos

$$A = \{1, 2, 3, 4\} \qquad \text{y} \qquad B = \{p, q, r, s\}$$

Ya que se han introducido las relaciones de orden, habrá tendencia aquí a poner el orden familiar al dar los elementos de cada conjunto. Lo indicamos para advertir al lector contra esto de atribuir a un conjunto cualquiera propiedades que no estén explícitamente establecidas. En (1) consideramos A y B como conjuntos arbitrarios de cuatro elementos cada uno y nada más; por ejemplo, podríamos escribir $\{*, +, \$, \%\}$ como A o como B; en (2) introducimos relaciones de orden sobre A y B pero no las mencionadas arriba; en (3) definimos operaciones binarias sobre los conjuntos no ordenados A y B; en (4) definimos operaciones binarias sobre los conjuntos ordenados de (2).

(1) La aplicación $\alpha: \quad 1 \leftrightarrow p,\ 2 \leftrightarrow q,\ 3 \leftrightarrow r,\ 4 \leftrightarrow s$

es una de las veinticuatro que establecen una biyección entre A y B.

(2) Sean A ordenado por la relación $\mathscr{R} = (\ |\ )$ y B ordenado por la relación $\mathscr{R}'$, como se indica en el diagrama de la Fig. 2-5. Como el diagrama para A es como se muestra en la Fig. 2-6, es claro que la aplicación

$$\beta: \quad 1 \leftrightarrow r,\ 2 \leftrightarrow s,\ 3 \leftrightarrow q,\ 4 \leftrightarrow p$$

es una biyección entre A y B que preserva las relaciones de orden; es decir, para cualesquiera $u, v \in A$ y $x, y \in B$ con $u \leftrightarrow x$ y $v \leftrightarrow y$ entonces

$$u \mathscr{R}' v \quad \text{implica} \quad x \mathscr{R} y$$

y recíprocamente.

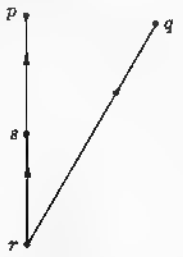


Fig. 2-5

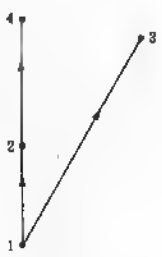


Fig. 2-6

(3) Defínanse en los conjuntos no ordenados A y B las operaciones binarias respectivas $\circ$ y $\square$ por las tablas de operación

A

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	t

Tabla 2-2

y

B

$\square$	p	q	r	s
p	q	r	s	p
q	r	s	p	q
r	s	p	q	r
s	p	q	r	s

Tabla 2-3

Se puede verificar fácilmente que la aplicación

$$\gamma: \quad 1 \leftrightarrow s,\ 2 \leftrightarrow p,\ 3 \leftrightarrow r,\ 4 \leftrightarrow q$$

es una biyección entre A y B que preserva las operaciones, es decir, que siempre que

$$w \in A \leftrightarrow x \in B \qquad \text{y} \qquad v \in A \leftrightarrow y \in B$$

(léase «w en A corresponde a x en B y v en A corresponde a y en B»), entonces

$$w \circ v \leftrightarrow x \square y$$

(4) Defínanse en los conjuntos ordenados A y B de (2) las respectivas operaciones binarias $\circ$ y $\square$ con las tablas de operación

A

$\circ$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabla 2-4

B

$\square$	p	q	r	s
p	r	s	p	q
q	s	p	q	r
r	p	q	r	s
s	q	r	s	p

Tabla 2-5

Se puede verificar fácilmente que la aplicación

$$\beta: \quad 1 \leftrightarrow r,\ 2 \leftrightarrow s,\ 3 \leftrightarrow q,\ 4 \leftrightarrow p$$

es una biyección entre A y B que preserva tanto las relaciones de orden como las operaciones.

Por *sistema algebraico* S entenderemos un conjunto S junto con cualesquiera relaciones y operaciones definidas sobre S. En cada uno de los casos (1)-(4) anteriores, se trata, pues, de una cierta correspondencia entre los conjuntos de los dos sistemas. En cada caso diremos que la aplicación de que se trata es un *isomorfismo* de A sobre B o que los sistemas A y B son isomorfos respecto de la aplicación; así, pues:

Dos sistemas S y T se dicen *isomorfos* si

(i) existe una biyección entre los conjuntos S y T, y
(ii) cualesquiera relaciones y operaciones definidas en los conjuntos se conservan en la biyección.

Consideremos con más detalle los dos sistemas A y B de (3). La operación binaria $\circ$ es asociativa y conmutativa; asimismo, con respecto a esta operación A tiene 1 como elemento neutro y todo elemento de A tiene simétrico. Es de sospechar que la Tabla 2-2 es algo más que un vacío ejercicio de construcción de un cuadro en que ningún elemento se presente dos veces en la misma fila o columna. Considerando los elementos de A como dígitos y no como símbolos abstractos, es fácil verificar que la operación binaria $\circ$ se puede definir así: para cualesquiera $x, y \in A$, $x \circ y$ es el resto de dividir $x \cdot y$ por 5. (Por ejemplo, $2 \cdot 4 = 8 = 1 \cdot 5 + 3$ y $2 \circ 4 = 3$.) Más aún, el sistema B no es más que una versión disfrazada o en clave del A, siendo la clave en este caso la biyección γ.

Emplearemos los isomorfismos entre sistemas algebraicos de dos maneras:

(*a*) Descubiertas ciertas propiedades de un sistema (por ejemplo, las de A enumeradas antes) podemos sin más trasladarlas como propiedades a cualquier otro sistema isomorfo con él.

(*b*) Siempre que sea más cómodo, podemos remplazar un sistema por otro isomorfo con él. Ejemplos de esto se encontrarán en los Capítulos 4 y 6.

PERMUTACIONES

Sea $S = \{1, 2, 3, \ldots, n\}$ y examínese el conjunto S_n de las $n!$ permutaciones de estos n símbolos. (No se da especial significación al hecho de que sean números naturales.) La definición de producto de composición de aplicaciones en el Capítulo 1 lleva naturalmente a definir una «operación permutación» $\circ$ entre los elementos de S_n. Ante todo vamos a introducir notaciones más cómodas para las permutaciones.

Sea $i_1, i_2, i_3, \ldots, i_n$ una cierta ordenación de los elementos de S. Usaremos una notación en dos líneas para la permutación

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}$$

que no es más que una variación de la notación para la aplicación

$$\alpha: \quad 1\alpha = i_1,\ 2\alpha = i_2,\ 3\alpha = i_3,\ \ldots,\ n\alpha = i_n$$

De igual modo, si $j_1, j_2, j_3, \ldots, j_n$ es otra ordenación de los elementos de S, escribiremos

$$\beta = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ j_1 & j_2 & j_3 & \ldots & j_n \end{pmatrix}$$

Por producto $\alpha \circ \beta$ entenderemos que α y β se han de hacer en ese orden. Así, pues, una reordenación de cualquier ordenación de los elementos de S es simplemente otra ordenación de éstos. De modo que para cualesquiera $\alpha, \beta \in S_n$, $\alpha \circ \beta \in S_n$ y entonces es $\circ$ una operación binaria sobre S_n.

Ejemplo 19: Sean $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}$, y $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$

tres de las 5! permutaciones del conjunto S_5 de todas las permutaciones de $S = \{1, 2, 3, 4, 5\}$.

Como el orden de las columnas en cualquier permutación no importa, se puede escribir también β como $\beta = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ en la que la línea superior de β es la inferior de α. Entonces

$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \circ \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$$

De igual modo, escribiendo α como $\begin{pmatrix} 1 & 3 & 2 & 5 & 4 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$, se encuentra que $\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$

De modo que $\circ$ no es conmutativa.

Escribiendo γ como $\begin{pmatrix} 3 & 2 & 5 & 4 & 1 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$, se tiene que

$$(\alpha \circ \beta) \circ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 3 & 2 & 5 & 4 & 1 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$$

Averigüe el lector $\beta \circ \gamma = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$ y compruebe que $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$. Así, pues, $\circ$ es asociativa en este ejemplo. Ahora es fácil demostrar que $\circ$ es asociativa sobre S_5 y también sobre S_n.

La permutación neutra o idéntica es $\mathcal{J} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ ya que evidentemente

$$\mathcal{J} \circ \alpha = \alpha \circ \mathcal{J} = \alpha, \quad \ldots$$

Por último, intercambiando las dos líneas de α, tenemos

$$\begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix} = \alpha^{-1}$$

pues $\alpha \circ \alpha^{-1} = \alpha^{-1} \circ \alpha = \mathcal{J}$. Además, es evidente que todo elemento de S_5 tiene un simétrico.

Se introduce ahora otra notación para las permutaciones. La permutación

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

del Ejemplo 19 se puede escribir en notación *cíclica* de la manera siguiente: (12345), interpretándose el ciclo (12345) como que 1 se cambia por 2, 2 se cambia por 3, 3 por 4, 4 por 5 y 5 por 1. La permutación

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

puede escribirse como (345), significando el ciclo (345) que 1 y 2, los símbolos que faltan, no se cam-

bian, en tanto que 3 se cambia por 4, 4 por 5 y 5 por 3. La permutación β se puede escribir (23)(45). La interpretación es clara: 1 no cambia; 2 se cambia por 3 y 3 por 2; 4 se remplaza por 5 y 5 por 4. Llamaremos a (23)(45) producto de ciclos. Nótese que estos ciclos son disjuntos, esto es, que no tienen símbolos en común. Así, pues, en notación cíclica es de esperar que una permutación de n símbolos consista en un solo ciclo o sea producto de dos o más ciclos mutuamente disjuntos. Claro que (23) y (45) son permutaciones de $S = \{1, 2, 3, 4, 5\}$ y, por tanto, $\beta = (23) \circ (45)$, pero seguiremos utilizando la yuxtaposición para indicar el producto de ciclos disjuntos. El lector verificará que $\alpha \circ \beta = (135)$ y que $\beta \circ \alpha = (124)$. En esta notación, la permutación idéntica o neutra $\mathscr{S}$ será denotada por (1).

Véase Problema 11.

TRANSPOSICIONES

Se llama *transposición* una permutación tal como la (12) o la (25), . . . , en que se intercambian solamente dos de los n símbolos de $S = \{1, 2, 3, \ldots, n\}$. Toda permutación se puede expresar, si bien no en forma única, como producto de transposiciones.

Ejemplo 20: Expresar las siguientes permutaciones:

$$(a)\ (23), \quad (b)\ (135), \quad (c)\ (2345), \quad (d)\ (12345)$$

en $S = \{1, 2, 3, 4, 5\}$ como resultado de las transposiciones

$$(a) \quad (23) = (12) \circ (23) \circ (13) = (12) \circ (13) \circ (12)$$

$$(b) \quad (135) = (13) \circ (15) = (15) \circ (35) = (15) \circ (13) \circ (15) \circ (13)$$

$$(c) \quad (2345) = (23) \circ (24) \circ (25) = (25) \circ (34) \circ (35)$$

$$(d) \quad (12345) = (12) \circ (13) \circ (14) \circ (15)$$

Este ejemplo ilustra el

Teorema V. Si una permutación α de n símbolos se expresa como producto de r transposiciones y asimismo como producto de s transposiciones, entonces r y s son ambos pares o ambos impares.

Para una demostración, véase Problema 12.

Una permutación se dice *par* (*impar*) si se puede expresar como producto de un número par (impar) de transposiciones. En el Problema 13 se demuestra el

Teorema VI. De las $n!$ permutaciones de n símbolos, la mitad son pares y la mitad impares.

El Ejemplo 20 ilustra también el

Teorema VII. Un ciclo de m símbolos se puede escribir como producto de $m - 1$ transposiciones.

SISTEMAS ALGEBRAICOS

Gran parte del resto de este libro se consagra al estudio de diversos sistemas algebraicos. Tales sistemas se pueden estudiar de una de estas dos maneras:

(*a*) Se empieza con un conjunto de elementos (por ejemplo, los números naturales o un conjunto isomorfo a éste), definiendo las operaciones binarias adición y multiplicación y derivando las leyes conocidas que rigen las operaciones con estos números.

(*b*) Se empieza con un conjunto S de elementos (no identificados); se define una operación binaria $\circ$; se establecen ciertos postulados, por ejemplo, que (i) $\circ$ es asociativa, que (ii) hay un elemento neutro, en S con respecto a $\circ$, (iii) que todo elemento de S tiene un simétrico respecto de $\circ$ en S; y se deducen los teoremas consiguientes.

Ambos procedimientos se ilustrarán aquí. En el capítulo próximo seguiremos el (*a*) al estudiar los números naturales.

Problemas resueltos

1. Demostrar que «es congruente con» en el conjunto T de los triángulos de un plano, es una relación de equivalencia.

(i) «a es congruente con a para todo $a \in T$» es cierto.

(ii) «Si a es congruente con b, entonces b es congruente con a», es cierto.

(iii) «Si a es congruente con b y b lo es con c, entonces a es congruente con c», es cierto.

Así, pues, «es congruente con» es una relación de equivalencia sobre T.

2. Demostrar que «$<$» en Z no es una relación de equivalencia.

(i) «$a < a$» para todo $a \in Z$ no es cierto.

(ii) «Si $a < b$, es $b < a$» tampoco es cierto.

(iii) «Si $a < b$ y $b < c$, entonces $a < c$» es cierto.

Así que «$<$» no es una relación de equivalencia en Z. (Nótese que (i) o (ii) es suficiente.)

3. Sea $\mathscr{R}$ una relación de equivalencia y supóngase que $c \mathscr{R} a$ y $c \mathscr{R} b$. Demostrar que $a \mathscr{R} b$.

Como $c \mathscr{R} a$, también $a \mathscr{R} c$ (por la propiedad simétrica). Como $a \mathscr{R} c$ y $c \mathscr{R} b$, entonces $a \mathscr{R} b$ (por la propiedad transitiva).

4. Demostrar que si $b \in [a]$, entonces $[b] = [a]$.

Sea $\mathscr{R}$ la relación de equivalencia que define $[a]$. Por definición, $b \in [a]$ implica $b \mathscr{R} a$ y $x \in [b]$ implica $x \mathscr{R} b$. Entonces $x \mathscr{R} a$ para todo $x \in [b]$ (por la propiedad transitiva) y $[b] \subseteq [a]$. Repitiendo el razonamiento con $a \mathscr{R} b$ (que resulta de la propiedad simétrica de $\mathscr{R}$) y $y \mathscr{R} a$ (siempre que $y \in [a]$) resulta $[a] \subseteq [b]$. Así, pues, $[b] = [a]$, como se afirmaba.

5. Demostrar que si $[a] \cap [b] \neq \varnothing$, entonces $[a] = [b]$.

Suponiendo que $[a] \cap [b] = \{r, s, \ldots\}$ se tiene $[r] = [a]$ y $[r] = [b]$ (por el Problema 4), y $[a] = [b]$ (por la propiedad transitiva de $=$).

6. Demostrar que una relación de equivalencia $\mathscr{R}$ sobre un conjunto S produce una partición de S y recíprocamente, una partición de S define una relación de equivalencia sobre S.

Sea $\mathscr{R}$ una relación de equivalencia sobre S y defínase para cada $p \in S$,

$$T_p = [p] = \{x:\ x \in S,\ x \mathscr{R} p\}$$

Como $p \in [p]$, es claro que S es la unión de todos los subconjuntos distintos $T_a, T_b, T_c, \ldots$ inducidos por $\mathscr{R}$. Pero para todo par de estos subconjuntos, como T_b y T_c, tenemos $T_b \cap T_c = \varnothing$ porque si no $T_b = T_c$, según el Problema 5. Así, pues, $\{T_a, T_b, T_c, \ldots\}$ es la partición de S efectuada por $\mathscr{R}$.

Recíprocamente, sea $\{T_a, T_b, T_c, \ldots\}$ una partición de S. Defínase sobre S la relación binaria $\mathscr{R}$ por $p \mathscr{R} q$ si, y solamente si, hay un T_i en la partición tal que $p, q \in T_i$. Es claro que $\mathscr{R}$ es reflexiva y simétrica. Supóngase $p \mathscr{R} q$ y $q \mathscr{R} r$; entonces, por la definición de $\mathscr{R}$, existen subconjuntos T_j y T_k (no necesariamente distintos) para los cuales $p, q \in T_j$ y $q, r \in T_k$. Pero como $T_j \cap T_k \neq \varnothing$, entonces $T_j = T_k$. Como $p, r \in T_j$, entonces $p \mathscr{R} r$ y $\mathscr{R}$ es transitiva. Así que $\mathscr{R}$ es una relación de equivalencia.

7. Hágase el diagrama del orden parcial de (*a*) el conjunto de subconjuntos de $S = \{a, b, c\}$ inducido por la relación binaria ($\subset$), (*b*) el conjunto $B = \{2, 4, 5, 8, 15, 45, 60\}$ inducido por la relación binaria (|).

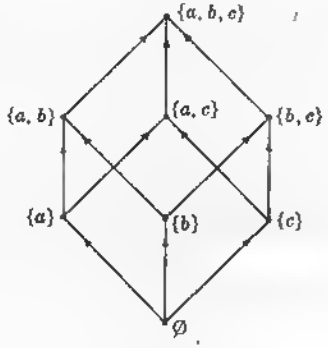


Fig. 2-7

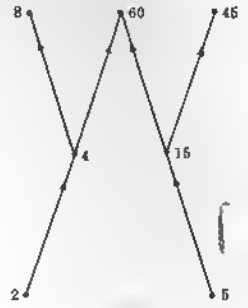


Fig. 2-8

Estas figuras no necesitan mayor elaboración una vez comprendido que se ha de emplear un número mínimo de segmentos. En la Fig. 2-7, por ejemplo, $\varnothing$ no se une directamente a $\{a, b, c\}$, puesto que $\varnothing \subseteq \{a, b, c\}$ viene indicado por el camino $\varnothing \subseteq \{a\} \subseteq \{a, b\} \subseteq \{a, b, c\}$. Análogamente, en la Fig. 2-8, los segmentos que unen 2 a 8 y 5 a 45 no son necesarios.

8. Demostrar que el elemento neutro, si existe, respecto de una operación binaria $\circ$ sobre un conjunto S es único.

Supóngase lo contrario, es decir, que q_1 y q_2 sean elementos neutros de S. Como q_1 es un elemento neutro, se tiene $q_1 \circ q_2 = q_2$, pero como q_2 también es elemento neutro, se tiene asimismo $q_1 \circ q_2 = q_1$. Así, pues, $q_1 = q_1 \circ q_2 = q_2$; y el elemento neutro es único.

9. Demostrar que la multiplicación es una operación binaria sobre $S = \{1, -1, i, -i\}$ siendo $i = \sqrt{-1}$.

La manera más simple de hacerlo es formar la tabla adyacente, notando que cada cabeza de línea o columna es un elemento único de S.

El orden en que se pongan los elementos de S encabezando las entradas es indiferente, pero siempre es algo ventajoso utilizar el mismo orden en ambos sentidos.

El lector puede demostrar fácilmente que la multiplicación sobre S es asociativa y conmutativa, que 1 es el elemento neutro y que los simétricos de $1, -1, i, -i$ son, respectivamente, $1, -1, -i, i$.

$\circ$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Tabla 2-6

10. Determinense las propiedades de las operaciones binarias $\circ$ y $\square$ definidas sobre $S = \{a, b, c, d\}$ por las tablas siguientes:

$\circ$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Tabla 2-7

$\square$	a	b	c	d
a	d	a	c	b
b	a	c	b	d
c	b	d	a	c
d	c	b	d	a

Tabla 2-8

La operación binaria $\circ$ definida por la Tabla 2-7 es conmutativa (verifíquese que las casillas están situadas simétricamente respecto de la diagonal principal) y asociativa (otra tarea). Hay un elemento neutro a (los encabezamientos de columna son también los elementos de la primera columna y los encabezamientos de fila son también los elementos de la primera fila). Los simétricos de a, b, c, d son, respectivamente, a, d, c, b ($a \circ a = b \circ d = c \circ c = d \circ b = a$).

La operación binaria $\square$ definida por la Tabla 2-8 no es conmutativa ($a \square c = c$, $c \square a = b$) ni asociativa ($a \square (b \square c) = a \square b = a$, $(a \square b) \square c = a \square c = c$). No hay elemento neutro y, por tanto, ningún elemento de S tiene simétrico.

Como $a \square (d \circ c) = a \neq d = (a \square d) \circ (a \square c)$ y $(d \circ c) \square a \neq (d \square a) \circ (c \square a)$, $\square$ no es distributiva ni a izquierda ni a derecha con respecto a $\circ$; como $d \circ (c \square b) = c \neq a = (d \circ c) \square (d \circ b)$ y $\circ$ es conmutativa, $\circ$ no es distributiva ni a izquierda ni a derecha con respecto a $\square$.

11. (*a*) Escribir las permutaciones (23) y (13)(245) con 5 símbolos en notación de dos líneas.
(*b*) Expresar los productos (23) $\circ$ (13)(245) y (13)(245) $\circ$ (23) en notación cíclica.
(*c*) Expresar en notación cíclica las simétricas de (23) y de (13)(245).

(*a*) $$(23) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} \quad \text{y} \quad (13)(245) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$$

(*b*) $$(23) \circ (13)(245) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 & 2 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix} = (13452)$$

y

$$(13)(245) \circ (23) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix} = (12453)$$

(*c*) La inversa de (23) es $\begin{pmatrix} 1 & 3 & 2 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = (23)$.

La inversa de (13)(245) es $\begin{pmatrix} 3 & 4 & 1 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = (13)(254)$.

12. Demostrar: Sea una permutación α de n símbolos expresada como producto de r transposiciones y también como producto de $s > r$ transposiciones. Entonces r y s son ambos pares o ambos impares.

Utilizando los símbolos diferentes $x_1, x_2, x_3, \ldots, x_n$, se forma el producto

$$\begin{aligned} A = {} & (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \cdots (x_1 - x_n) \\ & (x_2 - x_3)(x_2 - x_4) \cdots (x_2 - x_n) \\ & \cdots\cdots\cdots\cdots\cdots \\ & (x_{n-1} - x_n) \end{aligned}$$

Una transposición (u, v), donde $u < v$, sobre A tiene el efecto siguiente: (1) cualquier factor en que no entren ni x_u ni x_v permanece invariable, (2) solo el factor $x_u - x_v$ cambia de signo, (3) los restantes factores, los que contienen x_u o x_v, pero no ambos, se pueden agrupar en parejas, $(x_u - x_w)(x_v - x_w)$, donde $u < v < w$, $(x_u - x_w)(x_w - x_v)$ donde $u < w < v$ y $(x_w - x_u)(x_w - x_v)$ con $w < u < v$ todos los cuales permanecen invariables. Así, pues, el efecto de la transposición sobre A es cambiar su signo.

Ahora bien, el efecto de α sobre A es dar $(-1)^r A$ o $(-1)^s A$ según que α se escriba como producto de r o de s transposiciones. Como $(-1)^r A = (-1)^s A$, tenemos $A = (-1)^{s-r} A$, o sea que $s - r$ es par. Así, pues, r y s son ambos pares o ambos impares.

13. Demostrar que de las $n!$ permutaciones de n símbolos, la mitad son pares y la mitad impares.

Denótense las permutaciones pares por $p_1, p_2, p_3, \ldots, p_u$ y las impares por $q_1, q_2, q_3, \ldots, q_v$. Sea t una transposición cualquiera. Entonces $t \circ p_1, t \circ p_2, t \circ p_3, \ldots t \circ p_u$ son permutaciones de n símbolos, que son distintas porque $p_1, p_2, p_3, \ldots, p_u$ son distintas y son impares; así que $u \leq v$. También $t \circ q_1, t \circ q_2, t \circ q_3, \ldots, t \circ q_v$ son distintas y pares; así que $v \leq u$. Luego $u = v = \frac{1}{2}n!$

Problemas propuestos

14. ¿Cuáles de las siguientes son relaciones de equivalencia?

(*a*) «Es semejante a» para el conjunto T de todos los triángulos de un plano.

(*b*) «Tiene igual radio que» para todos los círculos de un plano.

(*c*) «Es el cuadrado de» para el conjunto N.

(*d*) «Tiene el mismo número de vértices que» para el conjunto de todos los polígonos de un plano.

(*e*) «$\subseteq$» para el conjunto de conjuntos $S = \{A, B, C, \ldots\}$.

(*f*) «$\leq$» para el conjunto R.

Resp. (*a*), (*b*), (*d*).

15. (*a*) Demostrar que «es factor de» en N es reflexiva y transitiva, pero no simétrica.

(*b*) Demostrar que «cuesta dólar más o menos» para zapatos de hombres es reflexiva y simétrica, pero no transitiva.

(*c*) Dar un ejemplo de relación simétrica y transitiva, pero no reflexiva.

(*d*) Deducir de (*a*), (*b*), (*c*) que dos propiedades de las reflexiva, simétrica, transitiva de una relación binaria no implican la otra.

16. Hacer el diagrama del orden parcial de

(*a*) $A = \{1, 2, 3, 6\}$

(*b*) $B = \{1, 2, 3, 5, 30, 60\}$ y (*c*) $C = \{1, 3, 5, 15, 30, 45\}$

inducida en cada uno por la relación ($|$).

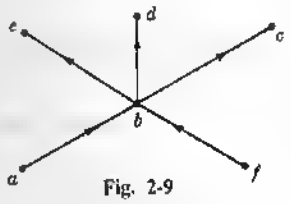


Fig. 2-9

17. Sea $S = \{a, b, c, d, e, f\}$ ordenado por la relación $\mathscr{R}$ como se ve en la Fig. 2-9. (*a*) Enumerar todos los pares $x, y \in S$ para los que $x \mathscr{R} y$. (*b*) Enumerar los subconjuntos de tres elementos que estén totalmente ordenados.

18. Verificar:

(*a*) el conjunto ordenado de subconjuntos de S en el Problema 7(*a*) tiene $\varnothing$ como primer elemento (también como elemento minimal) y S como último elemento (también como elemento maximal).

(*b*) el conjunto ordenado B del Problema 7(*b*) no tiene primero ni último elemento. ¿Cuáles son sus elementos minimal y maximal?.

(*c*) el subconjunto $C = \{2, 4, 5, 15, 60\}$ de B del Problema 7(*b*) carece de primero y último elemento. ¿Cuáles son sus elementos minimales y maximales?

19. Demostrar que:

(*a*) la multiplicación es una operación binaria sobre $S = \{1, -1\}$, pero no sobre $T = \{1, 2\}$.

(*b*) la adición es una operación binaria sobre $S = \{x: x \in Z, x < 0\}$, pero la multiplicación no.

20. Sea $S = \{A, B, C, D\}$ donde $A = \varnothing$, $B = \{a, b\}$, $C = \{a, c\}$, $D = \{a, b, c\}$. Constrúyanse tablas que muestren que $\cup$ es una operación binaria sobre S pero que $\cap$ no lo es.

21. Para las operaciones binarias $\circ$ y $\square$ definidas sobre $S = \{a, b, c, d, e\}$ por las Tablas 2-9 y 2-10, supóngase que son asociativas e investíguense todas las demás propiedades.

$\circ$	a	b	c	d	e
a	a	d	a	d	e
b	d	b	b	d	c
c	a	b	c	d	e
d	d	d	d	d	e
e	e	e	c	e	e

Tabla 2-9

$\square$	a	b	c	d	e
a	a	c	c	a	a
b	c	c	c	b	b
c	c	c	c	c	c
d	a	b	c	d	d
e	a	b	c	d	e

Tabla 2-10

22. Sea $S = \{A, B, C, D\}$ donde $A = \varnothing$, $B = \{a\}$, $C = \{a, b\}$, $D = \{a, b, c\}$.

(*a*) Constrúyanse tablas para demostrar que $\cup$ y $\cap$ son operaciones binarias sobre S.

(*b*) Supóngase la asociatividad para cada operación e investíguense todas las demás propiedades.

23. Para la operación binaria sobre $S = \{a, b, c, d, e, f, g, h\}$ definida por la Tabla 2-11, dése por sentada la asociatividad e investíguense todas las otras propiedades.

$\circ$	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	c	d	a	h	g	e	f
c	c	d	a	b	f	e	h	g
d	d	a	b	c	g	h	f	e
e	e	g	f	h	a	c	b	d
f	f	h	e	g	c	a	d	b
g	g	f	h	e	d	b	a	c
h	h	e	g	f	b	d	c	a

Tabla 2-11

24. Demuéstrese que $\circ$ definida en el Problema 23 es una operación binaria sobre los subconjuntos $S_0 = \{a\}$; $S_1 = \{a, c\}$, $S_2 = \{a, e\}$, $S_3 = \{a, f\}$, $S_4 = \{a, g\}$, $S_5 = \{a, h\}$, $S_6 = \{a, b, c, d\}$, $S_7 = \{a, c, e, f\}$, $S_8 = \{a, c, g, h\}$, pero no sobre los subconjuntos $T_1 = \{a, b\}$ y $T_2 = \{a, f, g\}$ de S.

25. Demostrar el Teorema IV. *Sugerencia*: Suponer que y y z son simétricos de x y considérese $z \circ (x \circ y) = (z \circ x) \circ y$.

26. (*a*) Demostrar que el conjunto N de los números naturales respecto de la adición y el conjunto $M = \{2x : x \in N\}$ respecto de la adición, son isomorfos. *Sugerencia*: Utilizar $n \in N \leftrightarrow 2n \in M$.
(*b*) El conjunto N respecto de la adición, ¿es isomorfo al conjunto $P = \{2x - 1 : x \in N\}$ respecto de la adición?
(*c*) El conjunto M de (*a*), ¿es isomorfo al conjunto P de (*b*)?

27. Sean A y B conjuntos dotados de las operaciones respectivas $\circ$ y $\square$. Supóngase que A y B son isomorfos y demuéstrese:
(*a*) Si la ley asociativa (conmutativa) se verifica en A, también se verifica en B.
(*b*) Si A tiene un elemento neutro u, entonces su correspondiente u' es el elemento neutro en B.
(*c*) Si cada elemento de A tiene un simétrico con respecto a $\circ$, lo mismo ocurre con los elementos de B respecto de $\square$.

Sugerencia: En (*a*), sea $a \in A \leftrightarrow a' \in B$, $b \leftrightarrow b'$, $c \leftrightarrow c'$. Entonces

$$a \circ (b \circ c) \leftrightarrow a' \square (b' \square c'), \qquad (a \circ b) \circ c \leftrightarrow (a' \square b') \square c'$$

y $$a \circ (b \circ c) = (a \circ b) \circ c \quad \text{implica} \quad a' \square (b' \square c') = (a' \square b') \square c'$$

28. Expresar cada una de las siguientes permutaciones de 8 símbolos como producto de ciclos disjuntos y como producto de transposiciones (en número mínimo).

(*a*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 5 & 6 & 7 & 8 \end{pmatrix}$ (*b*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix}$ (*c*) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 8 & 2 & 7 & 5 \end{pmatrix}$

(*d*) $(2468) \circ (348)$ (*e*) $(16)(2468) \circ (37)(15468)$ (*f*) $(135) \circ (3456) \circ (4678)$

Respuesta parcial. (*a*) $(1234) = (12)(13)(14)$

(*c*) $(13)(246)(58) = (13)(24)(26)(58)$

(*d*) $(28)(346) = (28)(34)(36)$

(*f*) $(1637845) = (16)(13)(17)(18)(14)(15)$

Nota: Por comodidad, $\circ$ se ha suprimido al indicar los productos de transposiciones.

29. Demostrar que los ciclos (1357) y (2468) del Problema 28(*b*) son conmutativos. Establecer el teorema correspondiente.

30. Escribir en notación cíclica las 6 permutaciones sobre $S = \{1, 2, 3\}$, denotarlas en cierto orden por $p_1, p_2, p_3, \ldots, p_6$ y formar una tabla de productos $p_i \circ p_j$.

31. Formar la tabla de operación (producto) para el conjunto $S = \{(1), (1234), (1432), (13)(24)\}$ de permutaciones de cuatro símbolos. Mediante la Tabla 2-3 mostrar que S es isomorfo a B.

Capítulo 3

Los números naturales

LOS POSTULADOS DE PEANO

Hasta ahora hemos supuesto las propiedades de los sistemas de números que son necesarias para proporcionarnos ejemplos y ejercicios en los primeros capítulos. En este capítulo nos proponemos construir el sistema de los números naturales suponiendo solamente unas cuantas de sus propiedades más simples. Estas propiedades más simples, conocidas como postulados (axiomas) de Peano, por el matemático italiano que los enunció en 1899, se pueden establecer como sigue:

Sea un conjunto N no vacío, tal que

Postulado I: $1 \in N$.

Postulado II: Para cada $n \in N$ existe un único $n^* \in N$, llamado *siguiente de* n.

Postulado III: Para cada $n \in N$ se tiene $n^* \neq 1$.

Postulado IV: Si $m, n \in N$ y $m^* = n^*$, entonces $m = n$.

Postulado V: Todo subconjunto K de N que tenga las propiedades

(a) $1 \in K$
(b) $k^* \in K$ siempre que $k \in K$

es el mismo N.

Primero veremos que, efectivamente, éstas son propiedades bien conocidas de los números naturales. Los Postulados I y II no requieren más explicación; el III establece que hay un primer número natural, el 1; el IV dice que distintos números naturales m y n tienen distintos siguientes $m + 1$ y $n + 1$; el V dice en esencia que cualquier número natural puede alcanzarse comenzando con 1 y contando los siguientes consecutivos.

Se observará que en las definiciones de adición y multiplicación sobre N que siguen no se acude a nada que sobrepase estos postulados.

ADICION SOBRE N

La adición sobre N se define por

(i) $n + 1 = n^*$ para todo $n \in N$.
(ii) $n + m^* = (n + m)^*$ siempre que $n + m$ esté definido.

Se demuestra que la adición está regida por las leyes siguientes:

Para cualesquiera $m, n, p \in N$,

A_1. Ley de clausura $n + m \in N$
A_2. Ley conmutativa $n + m = m + n$
A_3. Ley asociativa $m + (n + p) = (m + n) + p$
A_4. Ley de cancelación Si $m + p = n + p$, entonces $m = n$

MULTIPLICACION SOBRE N

La multiplicación se define por

(iii) $n \cdot 1 = n$.

(iv) $n \cdot m^* = n \cdot m + n$ siempre que $n \cdot m$ esté definido.

Se demuestra que la multiplicación se rige por las leyes siguientes:

Para cualesquiera $m, n, p \in N$

$\mathbf{M}_1$. Ley de clausura $n \cdot m \in N$

$\mathbf{M}_2$. Ley conmutativa $m \cdot n = n \cdot m$

$\mathbf{M}_3$. Ley asociativa $m \cdot (n \cdot p) = (m \cdot n) \cdot p$

$\mathbf{M}_4$. Ley de cancelación Si $m \cdot p = n \cdot p$, entonces $m = n$

La adición y la multiplicación siguen las leyes distributivas:

Para cualesquiera $m, n, p \in N$,

$\mathbf{D}_1$. $m \cdot (n + p) = m \cdot n + m \cdot p$

$\mathbf{D}_2$. $(n + p) \cdot m = n \cdot m + p \cdot m$

INDUCCION MATEMATICA

Sea la proposición

$$P(m): \quad m^* \neq m, \text{ para todo } m \in N$$

Demostraremos ahora cómo se puede establecer esta proposición solamente mediante los Postulados I-V. Definamos

$$K = \{k: k \in N, P(k) \text{ es cierto}\}$$

Como $1 \in N$ (Postulado I)

y $1^* \neq 1$ (Postulado III)

Entonces $P(1)$ es cierto y $1 \in K$

Sea ahora k cualquier elemento de K; entonces

(a) $$P(k): \quad k^* \neq k$$

es cierto. Pero si $(k^*)^* = k^*$ se sigue por el Postulado IV que $k^* = k$ en contradicción con (a). Por tanto,

$$P(k^*): \quad (k^*)^* \neq k^*$$

es verdadero y entonces $k^* \in K$. Así, pues, K tiene las dos propiedades enunciadas en el Postulado V; de modo que $K = N$ y la proposición es válida para todo $m \in N$.

Al establecer la validez de la proposición anterior, hemos probado al mismo tiempo el siguiente

Principio de inducción matemática

Una proposición $P(m)$ es cierta para todo $m \in N$ siempre que:

$P(1)$ sea cierto

y que para todo $k \in N$, $P(k)$ cierto implique $P(k^*)$ cierto

Las diferentes leyes $\mathbf{A}_1$-$\mathbf{A}_4$, $\mathbf{M}_1$-$\mathbf{M}_4$, $\mathbf{D}_1$-$\mathbf{D}_2$ se pueden basar en la inducción matemática. Así se establecen $\mathbf{A}_1$ en el Ejemplo 1, $\mathbf{A}_3$ en el Problema 1, $\mathbf{A}_2$ en los Problemas 2 y 3 y $\mathbf{D}_2$ en el Problema 5.

Ejemplo 1: Demostrar la ley de clausura: $n + m \in N$ para cualesquiera $m, n \in N$.

Tenemos que demostrar que $n + m$ está definido (es un número natural) por **(i)** y **(ii)** para cualesquiera n, $n \in N$. Supóngase que n sea cierto número natural fijo y considérese la proposición

$$P(m): \quad n + m \in N, \text{ para todo } m \in N$$

Como $$P(1): \quad n + 1 \in N$$

es cierto puesto que $n + 1 = n^*$ [por **(i)**] y $n^* \in N$ (por el Postulado II). Supóngase en seguida que para algún $k \in N$

$$(a) \qquad P(k): \quad n + k \in N \text{ es cierto}$$

se deduce entonces que $$P(k^*): \quad n + k^* \in N$$

es cierto puesto que $n + k^* = (n + k)^*$ (por **(ii)**) y $(n + k)^* \in N$ siempre que $n + k \in N$ (por el Postulado II). Así que, por inducción, $P(m)$ es cierto para todo $m \in N$ y como n era cualquier número natural, queda probada la ley de clausura para la adición.

En vista de las leyes de clausura $\mathbf{A}_1$ y $\mathbf{M}_1$, la adición y la multiplicación son (véase Capítulo 2) operaciones binarias sobre N. Las leyes $\mathbf{A}_3$ y $\mathbf{M}_3$ sugieren como definiciones para suma y producto de tres elementos $a_1, a_2, a_3 \in N$,

(v) $$a_1 + a_2 + a_3 = (a_1 + a_2) + a_3 = a_1 + (a_2 + a_3)$$

y

(vi) $$a_1 \cdot a_2 \cdot a_3 = (a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$$

Nótese que para una suma o producto de tres números naturales se pueden insertar paréntesis a voluntad. La suma de cuatro números naturales se examina en el Problema 4. El caso general se deja como ejercicio.

En el Problema 6 demostramos el

Teorema I. Todo elemento $n \neq 1$ de N es el siguiente de algún otro elemento de N.

RELACIONES DE ORDEN

Para cualesquiera $m, n \in N$ definimos «$<$» por

(vii) $m < n$ si, y solamente si, existe algún $p \in N$ tal que $m + p = n$.

En el Problema 8 se demuestra que la relación $<$ es transitiva, pero no reflexiva ni simétrica. Por el Teorema I,

$$1 < n \quad \text{para todo} \quad n \neq 1$$

y por **(i)** y **(vii)**, $$n < n^* \quad \text{para todo} \quad n \in N$$

Para cualesquiera $m, n \in N$ definimos «$>$» por

(viii) $m > n$ si, y solamente si, $n < m$

De aquí se sigue

La ley de tricotomía: Para cualesquiera $m, n \in N$ se verifica una, y solo una, de las siguientes relaciones:

$$(a) \quad m = n, \qquad (b) \quad m < n, \qquad (c) \quad m > n$$

Para una demostración, véase el Problema 10.

Otras consecuencias de las relaciones de orden son los Teoremas II y II':

Teorema II. Si $m, n \in N$ y $m < n$, entonces para todo $p \in N$

$$(a) \quad m + p < n + p \qquad (b) \quad m \cdot p < n \cdot p$$

y recíprocamente, si (a) o (b) son ciertas para algún $p \in N$, entonces $m < n$.

Teorema II'. Si $m, n \in N$ y $m > n$, entonces para todo $p \in N$

$$(a) \quad m + p > n + p$$
$$(b) \quad m \cdot p > n \cdot p$$

y reciprocamente, si (a) y (b) son ciertas para algún $p \in N$, entonces $m > n$.

Como el Teorema II' no es más que el Teorema II con m y n cambiadas, es claro que la demostración de una parte del Teorema II (véase Problema 11) demuestra la parte correspondiente del Teorema II'.

Las relaciones «menor o igual que» ($\preceq$) y «mayor o igual que» ($\succeq$) se definen como sigue:

Para $m, n \in N$, $\quad m \preceq n$ si $m < n$ o si $m = n$

$\quad m \succeq n$ si $m = n$ o si $m > n$

Sea A un subconjunto cualquiera de N (esto es, $A \subseteq N$). Un elemento p de A se dice *elemento mínimo* de A si $p \preceq a$ para todo $a \in A$. Nótese que en el lenguaje de los conjuntos, p es el primer elemento de A con respecto al orden $\preceq$. En el Problema 12 se demuestra el

Teorema III. El conjunto N es bien ordenado.

MULTIPLOS Y POTENCIAS

Sea $a \in S$, sobre el cual se han definido las operaciones binarias $+$ y $\cdot$, y hágase

$$1a = a \qquad a^1 = a$$

y

$$(k+1)a = ka + a \qquad a^{k+1} = a^k \cdot a$$

siempre que ka y a^k estén definidos para $k \in N$.

Ejemplo 2: Como $1a = a$ y $a^1 = a$, se tiene

$$2a = (1+1)a = 1a + 1a = a + a \quad \text{y} \quad a^2 = a^{1+1} = a^1 \cdot a = a \cdot a$$
$$3a = (2+1)a = 2a + 1a = a + a + a \quad \text{y} \quad a^3 = a^{2+1} = a^2 \cdot a = a \cdot a \cdot a$$
etc.

Debe tenerse en cuenta aquí que en el Ejemplo 2 el $+$ en $1 + 1$ y el $+$ en $a + a$ han de considerarse por completo distintos, pues el primero denota adición en N y el segundo en S. (Podría ser útil denotar las operaciones S por $\oplus$ y $\odot$.) En particular, $ka = a + a + \cdots + a$ es un múltiplo de a y se puede escribir como $k \cdot a$ solamente si $k \in S$.

Mediante el principio de inducción, se pueden demostrar las siguientes propiedades para cualesquiera $a, b \in S$ y cualesquiera $m, n \in N$:

(ix) $ma + na = (m+n)a$ **(ix)'** $a^m \cdot a^n = a^{m+n}$

(x) $m(na) = (m \cdot n)a$ **(x)'** $(a^n)^m = a^{m \cdot n}$

y, si $+$ y $\cdot$ son conmutativas sobre S,

(xi) $na + nb = n(a+b)$ **(xi)'** $a^n \cdot b^n = (ab)^n$

CONJUNTOS ISOMORFOS

Ya es evidente que el conjunto $\{1, 1^*, (1^*)^*, \ldots\}$ dotado de las operaciones y relaciones en él definidas, solo difiere por los símbolos empleados del familiar sistema $\{1, 2, 3, \ldots\}$ dotado de las operaciones y relaciones usuales. Si un romano hubiese escrito este capítulo es claro que habría llegado a la misma conclusión con su sistema $\{\text{I}, \text{II}, \text{III}, \ldots\}$. Se dice simplemente que los tres son isomorfos.

Problemas resueltos

1. Demostrar la ley asociativa A_3: $m + (n + p) = (m + n) + p$ para cualesquiera $m, n, p \in N$.

Sean m y n dos números naturales dados y considérese la proposición

$$P(p): \quad m + (n + p) = (m + n) + p \quad \text{para cualesquiera} \quad p \in N$$

Primero verificamos la validez de $P(1)$: $m + (n + 1) = (m + n) + 1$. Por (i) y (ii), página 30,

$$m + (n+1) = m + n^* = (m+n)^* = (m+n) + 1$$

y $P(1)$ es cierto.

En seguida, supóngase que para algún $k \in N$ se verifica

$$P(k): \quad m + (n + k) = (m + r) + k$$

Hay que demostrar que esto implica que

$$P(k^*): \quad m + (n + k^*) = (m + n) + k^*$$

es verdad. Por (ii), $\quad m + (n + k^*) = m + (n + k)^* = [m + (n + k)]^*$

y $\quad (m + n) + k^* = [(m + n) + k]^*$

Entonces, siempre que $P(k)$ sea cierto,

$$m + (n + k)^* = [m + (n + k)]^* = [(m + n) + k]^* = (m + n) + k^*$$

y $P(k^*)$ es cierto. Así, pues, $P(p)$ es cierto para todo $p \in N$ y como m y n son cualesquiera números naturales, queda demostrada A_3.

2. Demostrar que $P(n)$: $n + 1 = 1 + n$ para todo $n \in N$.

Evidentemente, $P(1) = 1 + 1 = 1 + 1$ es verdad. Supóngase ahora que para algún $k \in N$,

$$P(k): \quad k + 1 = 1 + k$$

sea cierto. Hay que demostrar que esto implica

$$P(k^*): \quad k^* + 1 = 1 + k^*$$

Mediante la aplicación sucesiva de la definición de k^*, de A_3, de la suposición que $P(k)$ es cierto, y de la definición de k^*, se tiene

$$1 + k^* = 1 + (k + 1) = (1 + k) + 1 = (k + 1) + 1 = k^* + 1$$

Así que $P(k^*)$ es cierto y queda demostrada $P(n)$.

3. Demostrar la ley conmutativa A_2: $m + n = n + m$ para todo $m, n \in N$.

Sea n un número natural dado, pero arbitrario, y considérese

$$P(m): \quad m + n = n + m \quad \text{para cualquiera} \quad m \in N$$

Por el Problema 2, $P(1)$ es cierto. Supóngase que para algún $k \in N$ se verifica

$$P(k): \quad k + n = n + k$$

Entonces

$$k^* + n = (k + 1) + n = k + (1 + n) = k + (n + 1) = k + n^* = (k + n)^* = (n + k)^* = n + k^*$$

Así, pues,

$$P(k^*): \quad k^* + n = n + k^*$$

es cierto y se sigue A_2.

El lector comprobará cuidadosamente que la sucesión de igualdades anterior se obtiene utilizando únicamente las definiciones, postulados, las leyes de la adición demostradas y, desde luego, la suposición básica de que $P(k)$ es cierto para algún valor arbitrario $k \in N$. Tanto en esta demostración como en las que vengan luego, se sobrentiende que cuando no se cite el porqué de un paso dado en la demostración, el lector ha de suplirlo.

4. (*a*) Sean $a_1, a_2, a_3, a_4 \in N$ y definase $a_1 + a_2 + a_3 + a_4 = (a_1 + a_2 + a_3) + a_4$. Demostrar que se pueden intercalar paréntesis a voluntad en $a_1 + a_2 + a_3 + a_4$.

Utilizando **(v)**, tenemos $a_1 + a_2 + a_3 + a_4 = (a_1 + a_2 + a_3) + a_4 = (a_1 + a_2) + a_3 + a_4 = (a_1 + a_2) + (a_3 + a_4) = a_1 + a_2 + (a_3 + a_4) = a_1 + (a_2 + a_3 + a_4)$, etc.

(*b*) Para $b, a_1, a_2, a_3 \in N$, mostrar que $b \cdot (a_1 + a_2 + a_3) = b \cdot a_1 + b \cdot a_2 + b \cdot a_3$.

$$b \cdot (a_1 + a_2 + a_3) = b \cdot [(a_1 + a_2) + a_3] = b \cdot (a_1 + a_2) + b \cdot a_3 = b \cdot a_1 + b \cdot a_2 + b \cdot a_3$$

5. Demostrar la ley distributiva $\mathbf{D}_2$: $(n + p) \cdot m = n \cdot m + p \cdot m$ para cualesquiera $m, n, p \in N$.

Supóngase dados n y p y considérese

$$P(m): \quad (n + p) \cdot m = n \cdot m + p \cdot m \text{ para todo } m \in N$$

Mediante $\mathbf{A}_1$ y **(iii)** se ve que es cierto

$$P(1): \quad (n + p) \cdot 1 = n + p = n \cdot 1 + p \cdot 1$$

Supóngase que para algún $k \in N$ se verifica

$$P(k): \quad (n + p) \cdot k = n \cdot k + p \cdot k$$

Entonces

$$\begin{aligned}(n + p) \cdot k^* &= (n + p) \cdot k + (n + p) = n \cdot k + p \cdot k + n + p \\ &= n \cdot k + (p \cdot k + n) + p = n \cdot k + (n + p \cdot k) + p \\ &= (n \cdot k + n) + (p \cdot k + p) = n \cdot k^* + p \cdot k^*\end{aligned}$$

Así, pues

$$P(k^*): \quad (n + p) \cdot k^* = n \cdot k^* + p \cdot k^*$$

es cierto y queda demostrada $\mathbf{D}_2$.

6. Demostrar que: Todo elemento $n \neq 1$ de N es el siguiente de algún otro elemento de N.

Primero observamos que el Postulado III excluye el 1 como siguiente. Denótese por K el conjunto formado por el elemento 1 y todos los elementos de N que son siguientes, es decir,

$$K = \{k;\ k \in N,\ k = 1 \text{ o } k = m^* \text{ para algún } m \in N\}$$

Pero todo $k \in K$ tiene un siguiente único, $k^* \in N$ (Postulado II) y como k^* es un siguiente, tenemos $k^* \in K$. Entonces $K = N$ (Postulado V). Luego, para todo $n \in N$ se tiene o bien $n = 1$, o bien $n = m^*$ para algún $m \in N$.

7. Demostrar: $m + n \neq m$ para cualesquiera $m, n \in N$.

Sea n un número dado y considérese $P(m)$: $m + n \neq m$ para todo $m \in N$. Por el Postulado III, $P(1)$: $1 + n \neq 1$ es cierto. Supóngase que para algún $k \in N$ se verifica

(*a*) $$P(k): \quad k + n \neq k$$

Ahora bien, $(k + n)^* \neq k^*$ pues por el Postulado IV, $(k + n)^* = k^*$ implica $k + n = k$ en contradicción con (*a*). Así, pues,

$$P(k^*): \quad k^* + n \neq k^*$$

es cierto y el teorema queda demostrado.

8. Demostrar que $<$ es transitiva, pero no reflexiva ni simétrica.

Sean $m, n, p \in N$ y supóngase que $m < n$ y $n < p$. Por **(vii)**, existen $r, s \in N$ tales que $m + r = n$ y $n + s = p$. Entonces

$$n + s = (m + r) + s = m + (r + s) = p$$

Con lo que $m < p$ y $<$ es transitiva.

Sea $n \in N$. Ahora bien, $n < n$ es falso, pues si fuera cierto, existiría algún $k \in N$ tal que $n + k = n$ en contra del resultado obtenido en el Problema 7. Así, pues, $<$ no es reflexiva.

Finalmente, sean $m, n \in N$ y supóngase $m < n$ y $n < m$. Como $<$ es transitiva, se sigue que $m < m$ en contradicción con lo visto en el párrafo anterior. Así que $<$ no es simétrica.

9. Demostrar que $1 \leq n$ para todo $n \in N$.

Si $n = 1$, la igualdad se verifica; para otro caso, por el Problema 6, $n = m^* = m + 1$, para algún $m \in N$ y se tiene la desigualdad.

10. Demostrar la ley de tricotomía: Para cualesquiera $m, n \in N$ se verifica una de las siguientes relaciones y solo una

$$(a)\ m = n \qquad (b)\ m < n \qquad (c)\ m > n$$

Sea m cualquier elemento de N y constrúyanse los subconjuntos

$$N_1 = \{m\}, \qquad N_2 = \{x:\ x \in N,\ x < m\}, \qquad N_3 = \{x:\ x \in N,\ x > m\}$$

Vamos a demostrar que $\{N_1, N_2, N_3\}$ es una partición de N con respecto a $\{=, <, >\}$.

(1) Supóngase $m = 1$; entonces $N_1 = \{1\}$, $N_2 = \varnothing$ (Problema 9) y $N_3 = \{x:\ x \in N,\ x > 1\}$. Es claro que $N_1 \cup N_2 \cup N_3 = N$. Para completar, pues, la demostración en este caso, solo queda por comprobar que $N_1 \cap N_2 = N_1 \cap N_3 = N_2 \cap N_3 = \varnothing$.

(2) Supóngase $m \neq 1$. Como $1 \in N_2$, se sigue que $1 \in N_1 \cup N_2 \cup N_3$. Tómese ahora cualquier $n \neq 1 \in N_1 \cup N_2 \cup N_3$. Hay tres casos posibles por examinar:

(i) $n \in N_1$. Aquí, $n = m$ y entonces $n^* \in N_3$.

(ii) $n \in N_2$ demostrar que $n + p = m$ para algún $p \in N$. Si $p = 1$, es $n^* = m \in N_1$; si $p \neq 1$ de modo que $p = 1 + q$ para algún $q \in N$, es $n^* + q = m$ y entonces $n^* \in N_2$.

(iii) $n \in N_3$. Aquí $n^* > n > m$ y así $n^* \in N_3$.

Por consiguiente, para todo $n \in N$,

$$n \in N_1 \cup N_2 \cup N_3 \quad \text{implica} \quad n^* \in N_1 \cup N_2 \cup N_3$$

Como $1 \in N_1 \cup N_2 \cup N_3$ se concluye que $N = N_1 \cup N_2 \cup N_3$.

Ahora bien, $m \notin N_2$, porque $m \not< m$; luego $N_1 \cap N_2 = \varnothing$. Del mismo modo, $m \not> m$, y entonces $N_1 \cap N_2 = \varnothing$. Supóngase que $N_2 \cap N_3 = \{p\}$ para algún $p \in N$. Entonces, $p < m$ y $p > m$ o, lo que es lo mismo, $p < m$ y $m < p$. Como $<$ es transitiva tenemos $p < p$, que es una contradicción. Así, pues, hemos de concluir que $N_2 \cap N_3 = \varnothing$ y la demostración queda completa para este caso.

11. Demostrar que: si $m, n \in N$ y $m < n$, entonces para todo $p \in N$, $m + p < n + p$ y recíprocamente.

Como $m < n$ existe algún $k \in N$ tal que $m + k = n$. Luego

$$n + p = (m + k) + p = m + k + p = m + p + k = (m + p) + k$$

y entonces

$$m + p < n + p$$

Para la recíproca, supóngase $m + p < n + p$. Entonces, o bien $m = n$, o bien $m < n$, o bien $m > n$. Si $m = n$, entonces $m + p = n + p$; si $m > n$, entonces $m + p > n + p$ (Teorema 11') Como esto contradice la hipótesis, se concluye que $m < n$.

12. Demostrar que el conjunto N es bien ordenado.

Sea un subconjunto cualquiera $S \neq \varnothing$ de N. Hay que demostrar que S tiene un elemento mínimo. Esto es cierto si $1 \in S$. Supóngase que $1 \notin S$; entonces $1 < s$ para todo $s \in S$. Designese por K el conjunto

$$K = \{k:\ k \in N,\ k \leq s \text{ para todo } s \in S\}$$

Como $1 \in K$, entonces $K \neq \varnothing$. Además, $K \neq N$; por tanto, debe existir un $r \in K$ tal que $r^* \notin K$. Pero este $r \in S$, pues si no, $r < s$, y entonces $r^* \leq s$ para todo $s \in S$. Pero con ello se tendría $r^* \in K$, en contradicción con lo supuesto respecto de r. Así que S tiene un elemento mínimo. Y como S era cualquier subconjunto no vacío de N, se tiene, pues, que todo subconjunto no vacío de N tiene un elemento mínimo y, por tanto, N es bien ordenado.

Problemas propuestos

13. Demostrar por inducción: $1 \cdot n = n$ para todo $n \in N$.

14. Demostrar por inducción: (*a*) M_1, (*b*) M_2, (*c*) M_3.
Sugerencia: Utilizar el resultado del Problema 13 y D_2 en (*b*).

15. Demostrar: (*a*) D_1 siguiendo el Problema 5, (*b*) D_1 mediante M_2.

16. Demostrar: (*a*) $(m+n^*)^* = m^* + n^*$
(*b*) $(m \cdot n^*)^* = m \cdot n + m^*$
(*c*) $(m^* \cdot n^*)^* = m^* + m \cdot n + n^*$
siendo $m, n \in N$.

17. Demostrar: (*a*) $(m+n) \cdot (p+q) = (m \cdot p + m \cdot q) + (n \cdot p + n \cdot q)$
(*b*) $m \cdot (n+p) \cdot q = (m \cdot n) \cdot q + m \cdot (p \cdot q)$
(*c*) $m^* + n^* = (m+n)^* + 1$
(*d*) $m^* \cdot n^* = (m \cdot n)^* + m + n$

18. Sean $m, n, p, q \in N$ y defínase $m \cdot n \cdot p \cdot q = (m \cdot n \cdot p) \cdot q$. (*a*) Demostrar que se pueden intercalar paréntesis a voluntad en $m \cdot n \cdot p \cdot q$. (*b*) Demostrar que $m \cdot (n + p + q) = m \cdot n + m \cdot p + m \cdot q$.

19. Identifíquese $S = \{x: x \in N,\ n < x < n^*$ para todo $n \in N\}$.

20. Si $m, n, p, q \in N$ y si $m < n$ y $p < q$ demostrar: (*a*) $m + p < n + q$, (*b*) $m \cdot p < n \cdot q$.

21. Sean $m, n \in N$. Demostrar: (*a*) Si $m = n$, entonces $k^* \cdot m > n$ para todo $k \in N$. (*b*) Si $k^* \cdot m = n$ para algún $k \in N$, entonces $m < n$.

22. Demostrar A_4 y M_4 con la ley de tricotomía y los Teoremas 11, página 32, y 13, página 33.

23. Para todo $m \in N$ definir $m^1 = m$ y $m^{p+1} = m^p \cdot m$ siempre que m^p esté definido. Si $m, n, p, q \in N$, demuéstrese: (*a*) $m^p \cdot m^q = m^{p+q}$, (*b*) $(m^p)^q = m^{p \cdot q}$, (*c*) $(m \cdot n)^p = m^p \cdot n^p$, (*d*) $(1)^p = 1$.

24. Con $m, n \in N$ mostrar que (*a*) $m^2 < m \cdot n < n^2$ si $m < n$, (*b*) $m^2 + n^2 > 2m \cdot n$ si $m \neq n$.

25. Demostrar por inducción que para todo $n \in N$:
(*a*) $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n+1)$
(*b*) $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$
(*c*) $1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{1}{4}n^2(n+1)^2$

26. Con $a_1, a_2, a_3, \ldots, a_n \in N$ defínase $a_1 + a_2 + a_3 + \cdots + a_k = (a_1 + a_2 + a_3 + \cdots + a_{k-1}) + a_k$ para $k = 3, 4, 5, \ldots, n$. Demostrar:
(*a*) $a_1 + a_2 + a_3 + \cdots + a_n = (a_1 + a_2 + a_3 + \cdots + a_r) + (a_{r+1} + a_{r+2} + a_{r+3} + \cdots + a_n)$
(*b*) En una suma de n números naturales se pueden intercalar paréntesis a voluntad.

27. Demostrar cada una de las siguientes formas diversas del principio de inducción.
(*a*) Sea una proposición $P(n)$ asociada a cada $n \in N$. Entonces $P(n)$ es cierta para todo $n \in N$ si:
(i) $P(1)$ es cierto.
(ii) Para todo $m \in N$ la suposición de que $P(k)$ es cierta para todo $k < m$, implica que $P(m)$ es cierta.

(*b*) Sea b un cierto número natural dado, y sea una proposición $P(n)$ asociada con cada número natural $n \geq b$. Entonces $P(n)$ es cierta para todos los valores de n siempre que:
(i) $P(b)$ sea cierta.
(ii) Para todo $m > b$ la suposición de que $P(k)$ es cierta para todo $k \in N$ tal que $b \leq k < m$ implique $P(m)$ es cierta.

Capítulo 4

Los enteros

INTRODUCCION

El sistema de los números naturales tiene un defecto manifiesto en que dados $m, s \in N$, la ecuación $m + x = s$ puede tener o no tener solución. Por ejemplo, $m + x = m$ carece de solución (véase Problema 7, Capítulo 3), mientras que la $m + x = m^*$ tiene la solución $x = 1$. Es sabido que esto se remedia añadiendo a los números naturales (llamados entonces enteros positivos) el cero y los enteros negativos para formar el conjunto Z de los números enteros.

En este capítulo se muestra cómo puede construirse el sistema de los enteros a partir del sistema de los números naturales. Con tal fin se forma el conjunto producto

$$L = N \times N = \{(s, m) : s \in N, m \in N\}$$

No se dirá ahora, por ejemplo, (s, m) es una solución de $m + x = s$. Pero quede claro que se procede como si ése fuera el caso. Nótese que si (s, m) fuera solución de $m + x = s$, entonces (s, m) sería también solución de $m^* + x = s^*$, que a su vez tendría como solución (s^*, m^*). Esta observación sugiere la partición de L en clases de equivalencia tales que (s, m) y (s^*, m^*) sean elementos de la misma clase.

RELACION BINARIA $\sim$

Sea la relación binaria «$\sim$», léase «equivalente», definida para cualesquiera $(s, m), (t, n) \in L$ por

$$(s, m) \sim (t, n) \quad \text{si, y solo si,} \quad s + n = t + m$$

Ejemplo 1:
(a) $(5, 2) \sim (9, 6)$ pues $5 + 6 = 9 + 2$
(b) $(5, 2) \not\sim (8, 4)$ pues $5 + 4 \neq 8 + 2$
(c) $(r, r) \sim (s, s)$ pues $r + s = s + r$
(d) $(r^*, r) \sim (s^*, s)$ pues $r^* + s = s^* + r$
(e) $(r^*, s^*) \sim (r, s)$ pues $r^* + s = r + s^*$
siempre que $r, s \in N$.

Entonces $\sim$ es una relación de equivalencia (véase Problema 1) que induce en L una partición en clases de equivalencia $\mathscr{S} = \{[s, m], [t, n], \ldots\}$ donde

$$[s, m] = \{(a, b) : (a, b) \in L, (a, b) \sim (s, m)\}$$

Recordemos del Capítulo 2 que $(s, m) \in [s, m]$ y que si $(c, d) \in [s, m]$, entonces $[c, d] = [s, m]$. Así, pues,

$$[s, m] = [t, n] \quad \text{si, y solo si,} \quad (s, m) \sim (t, n)$$

Vamos a demostrar ahora que el conjunto $\mathscr{S}$ de clases de equivalencia de L respecto de $\sim$ es, aparte los símbolos empleados, el conjunto ya conocido Z de los enteros.

ADICION Y MULTIPLICACION SOBRE $\mathscr{J}$

La adición y la multiplicación sobre $\mathscr{J}$ se definirán, respectivamente, por

$$\text{(i)} \qquad [s,m] + [t,n] = [(s+t),\ (m+n)]$$

$$\text{(ii)} \qquad [s,m] \cdot [t,n] = [(s \cdot t + m \cdot n),\ (s \cdot n + m \cdot t)]$$

para cualesquiera $[s,m], [t,n] \in \mathscr{J}$.

La inspección de los segundos miembros de (i) y (ii) muestra que se cumplen las leyes de clausura

$\mathbf{A}_1$. $\quad x + y \in \mathscr{J}$ para cualesquiera $x, y \in \mathscr{J}$

y

$\mathbf{M}_1$. $\quad x \cdot y \in \mathscr{J}$ para cualesquiera $x, y \in \mathscr{J}$

En el Problema 3 se demuestra el

Teorema I. La clase de equivalencia a la que pertenece la suma (producto) de dos elementos pertenecientes a sendas clases de equivalencia de $\mathscr{J}$ es independiente de los elementos particulares elegidos.

Ejemplo 2: Si $(a,b), (c,d) \in [s,m]$ y $(e,f), (g,h) \in [t,n]$, no solo se tiene

$$[a,b] = [c,d] = [s,m] \qquad \text{y} \qquad [e,f] = [g,h] = [t,n]$$

sino también por el Teorema I

$$[a,b] + [e,f] = [c,d] + [g,h] = [s,m] + [t,n]$$

y

$$[a,b] \cdot [e,f] = [c,d] \cdot [g,h] = [s,m] \cdot [t,n]$$

El Teorema I también se puede enunciar como sigue: La adición y la multiplicación sobre $\mathscr{J}$ son compatibles con la relación de equivalencia y, por tanto, *bien definidas*.

Mediante las leyes conmutativa y asociativa para la adición y la multiplicación sobre N, no es difícil demostrar que la adición y la multiplicación sobre $\mathscr{J}$ obedecen a las mismas leyes. La ley asociativa para la adición y una de las leyes distributivas se demuestran en los Problemas 4 y 5.

LOS ENTEROS POSITIVOS

Sea $r \in N$. De $1 + r = r^*$ se sigue que r es solución de $1 + x = r^*$. Considérese ahora la aplicación

$$[n^*, 1] \leftrightarrow n, \quad n \in N \tag{1}$$

Para esta transformación encontramos

$$[r^*,1] + [s^*,1] = [(r^* + s^*),\ (1+1)] = [(r+s)^*, 1] \leftrightarrow r + s$$

y

$$[r^*,1] \cdot [s^*,1] = [(r^* \cdot s^* + 1 \cdot 1),\ (r^* \cdot 1 + s^* \cdot 1)] = [(r \cdot s)^*, 1] \leftrightarrow r \cdot s$$

Así que (1) es un isomorfismo del subconjunto $\{[n^*, 1]: n \in N\}$ de $\mathscr{J}$ sobre N.

Supóngase ahora que $[s,m] = [r^*, 1]$. Entonces $(s,m) \sim (r^*, 1)$, $s = r + m$ y $s > m$. Lo cual sugiere definir el conjunto Z^+ de los enteros positivos por

$$Z^+ = \{[s,m]: [s,m] \in \mathscr{J},\ s > m\}$$

En vista del isomorfismo (1) el conjunto Z^+ puede sustituirse por el conjunto N donde quiera que este último resulte más cómodo.

EL CERO Y LOS ENTEROS NEGATIVOS

Sean $r, s \in N$. Se tiene que $[r, r] = [s, s]$ para cualesquiera r y s y $[r, r] = [s, t]$ si, y solo si, $t = s$. Definimos el entero *cero*, 0, como el que corresponde a la clase de equivalencia $[r, r]$, $r \in N$. Sus propiedades conocidas son

$$[s, m] + [r, r] = [s, m] \qquad \text{y} \qquad [s, m] \cdot [r, r] = [r, r]$$

demostradas en los Problemas 2(*b*) y 2(*c*). La primera de éstas es la que lleva a designar el cero como elemento neutro de la adición.

Por último, definimos el conjunto Z^- de los enteros negativos por

$$Z^- = \{[s, m]: [s, m] \in \mathscr{J},\ s < m\}$$

Se sigue ahora que para cada entero $[a, b]$, $a \neq b$ existe un único entero $[b, a]$ tal que [véase Problema 2(*d*)]

$$[a, b] + [b, a] = [r, r] \leftrightarrow 0 \tag{2}$$

Se denota $[b, a]$ por $-[a, b]$ y se le llama *opuesto* de $[a, b]$. La relación (2) sugiere la designación $[b, a]$ o $-[a, b]$ como el *simétrico aditivo* de $[a, b]$.

LOS ENTEROS

Sean $p, q \in N$. Por la ley de tricotomía para los números naturales, hay tres posibilidades

(*a*) $p = q$, de donde $[p, q] = [q, p] \leftrightarrow 0$.

(*b*) $p < q$, de modo que $p + a = q$ para cualquiera $a \in N$; entonces $p + a^* = q + 1$ y $[q, p] = [a^*, 1] \leftrightarrow a$.

(*c*) $p > q$, de modo que $p = q + a$ para cualquiera $a \in N$ y $[p, q] \leftrightarrow a$.

Supóngase que $[p, q] \leftrightarrow n \in N$. Como $[q, p] = -[p, q]$, introduciremos el símbolo $-n$ para denotar el opuesto de $n \in N$ y escribiremos $[q, p] \leftrightarrow -n$. Así, cada clase de equivalencia de $\mathscr{J}$ se aplica ahora sobre un elemento único de $Z = \{0, \pm 1, \pm 2, \ldots\}$. Que $\mathscr{J}$ y Z son isomorfos se sigue inmediatamente una vez establecidas las propiedades conocidas del signo menos. Sin embargo, al demostrar la mayoría de las propiedades fundamentales de los enteros, suele ser conveniente el utilizar las correspondientes clases de equivalencia de

Ejemplo 3: Sean $a, b \in Z$. Mostrar que $(-a) \cdot b = -(a \cdot b)$. Sea $a \leftrightarrow [s, m]$ de modo que $-a \leftrightarrow [m, s]$ y sea $b \leftrightarrow [t, n]$. Entonces

$$(-a) \cdot b \leftrightarrow [m, s] \cdot [t, n] = [(m \cdot t + s \cdot n), (m \cdot n + s \cdot t)]$$

y

$$a \cdot b \leftrightarrow [s, m] \cdot [t, n] = [(s \cdot t + m \cdot n), (s \cdot n + m \cdot t)]$$

Como

$$-(a \cdot b) \leftrightarrow [(s \cdot n + m \cdot t), (s \cdot t + m \cdot n)] \leftrightarrow [(-a) \cdot b]$$

resulta que

$$(-a) \cdot b = -(a \cdot b)$$

Véanse Problemas 6-7.

RELACIONES DE ORDEN

Para $a, b \in Z$, sea $a \leftrightarrow [s, m]$ y $b \leftrightarrow [t, n]$. Las relaciones de orden «<» y «>» entre los enteros se definen por

$$a < b \quad \text{si, y solo si,} \quad (s + n) < (t + m)$$

y

$$a > b \quad \text{si, y solo si,} \quad (s + n) > (t + m)$$

En el Problema 8 se demuestra la *ley de tricotomía*: para cualesquiera $a, b \in Z$, se verifica una, y solo una, de las siguientes relaciones

$$(a)\ a = b, \qquad (b)\ a < b, \qquad (c)\ a > b$$

Si $a, b, c \in Z$, se tiene:

(1) $a + c < b + c$ si, y solo si, $a < b$.

(1') $a + c > b + c$ si, y solo si, $a > b$.

(2) Si $c > 0$, es $a \cdot c < b \cdot c$ si, y solo si, $a < b$.

(2') Si $c > 0$, es $a \cdot c > b \cdot c$ si, y solo si, $a > b$.

(3) Si $c < 0$, es $a \cdot c < b \cdot c$ si, y solo si, $a > b$.

(3') Si $c < 0$, es $a \cdot c > b \cdot c$ si, y solo si, $a < b$.

Para las demostraciones de (1') y (3), véanse Problemas 9-10.

La ley de cancelación para la multiplicación sobre Z,

$\mathbf{M_4}$. Si $z \neq 0$ y si $x \cdot z = y \cdot z$, es $x = y$

puede demostrarse ahora.

Como consecuencia inmediata, se tiene el

Teorema II. Si $a, b \in Z$ y si $a \cdot b = 0$, entonces o bien $a = 0$ o bien $b = 0$.

Para una demostración, véase Problema 11.

Las relaciones de orden permiten escribir los enteros en el orden acostumbrado

$$\ldots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \ldots$$

y su representación por puntos igualmente espaciados en una recta. Entonces «$a < b$» significa «a está a la izquierda de b» y «$a > b$» significa «a está a la derecha de b».

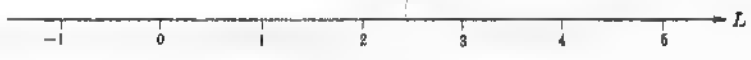


Fig. 4-1

De esta ordenación de los enteros se infiere el

Teorema III. No existe ningún $n \in Z^+$ tal que $0 < n < 1$.

Este teorema (véase Problema 12 para una demostración) es una consecuencia del hecho de que el conjunto Z^+ de los enteros positivos (por ser isomorfo al N) es bien ordenado.

SUSTRACCION «−»

Se define en Z la sustracción «−» por $a - b = a + (-b)$. La sustracción es evidentemente una operación binaria sobre Z. Sin embargo, no es conmutativa ni asociativa, si bien la multiplicación es distributiva respecto de la sustracción.

Ejemplo 4: Demostrar: $a - (b - c) \neq (a - b) - c$ con $a, b, c \in Z$ y $c \neq 0$.

Sean $a \leftrightarrow [s, m]$, $b \leftrightarrow [t, n]$, y $c \leftrightarrow [u, p]$. Entonces,

$$b - c = b + (-c) \leftrightarrow [(t + p), (n + u)]$$

$$-(b - c) \leftrightarrow [(n + u), (t + p)]$$

y $$a - (b - c) = a + (-(b - c)) \leftrightarrow [(s + n + u), (m + t + p)]$$

pero $$a - b = a + (-b) \leftrightarrow [(s + n), (m + t)]$$

y $$(a - b) - c = (a + b) + (-c) \leftrightarrow [(s + n + p), (m + t + u)]$$

Así que, con $c \neq 0$, $a - (b - c) \neq (a - b) - c$.

VALOR ABSOLUTO $|a|$

Se define el valor absoluto «$|a|$» de un entero a por

$$|a| = \begin{cases} a & \text{si} \quad a \geq 0 \\ -a & \text{si} \quad a < 0 \end{cases}$$

Así, pues, excepto cuando $a = 0$, $|a| \in Z^+$.

Cuando al menos uno de los a, b es 0, las siguientes leyes son evidentes

(1)	$-\|a\| \leq a \leq \|a\|$	(2)	$\|a \cdot b\| = \|a\| \cdot \|b\|$
(3)	$\|a\| - \|b\| \leq \|a + b\|$	(3′)	$\|a + b\| \leq \|a\| + \|b\|$
(4)	$\|a\| - \|b\| \leq \|a - b\|$	(4′)	$\|a - b\| \leq \|a\| + \|b\|$

Se pueden demostrar para cualesquiera $a, b \in Z$ considerando los casos separados en los Problemas 14 y 15.

ADICION Y MULTIPLICACION SOBRE Z

Las operaciones de adición y multiplicación sobre Z siguen las leyes $\mathbf{A}_1$-$\mathbf{A}_4$, $\mathbf{M}_1$-$\mathbf{M}_4$ y $\mathbf{D}_1$-$\mathbf{D}_2$ del Capítulo 3 (enunciadas para enteros) con la única modificación siguiente:

$\mathbf{M}_4$. **Ley de cancelación:** Si $m \cdot p = n \cdot p$ y si $p \neq 0 \in Z$, entonces $m = n$ para cualesquiera $m, n \in Z$.

He aquí dos propiedades de Z que no tenía N:

$\mathbf{A}_5$. Existe un elemento neutro, $0 \in Z$ para la adición, tal que $n + 0 = 0 + n = n$ para todo $n \in Z$.

$\mathbf{A}_6$. Para todo $n \in Z$ existe un simétrico aditivo, $-n \in Z$, tal que $n + (-n) = (-n) + n = 0$ y que se llama opuesto de n y otra propiedad común a N y Z.

$\mathbf{M}_5$. Existe un elemento neutro, $1 \in Z$, respecto de la multiplicación, tal que $1 \cdot n = n \cdot 1 = n$ para todo $n \in Z$.

Por el Teorema III, Capítulo 2, el elemento neutro en $\mathbf{A}_5$ y el elemento neutro en $\mathbf{M}_5$ son únicos; por el Teorema IV, Capítulo 2, cada simétrico aditivo en $\mathbf{A}_6$ es único.

OTRAS PROPIEDADES DE LOS ENTEROS

Ciertas propiedades de los enteros se han establecido mediante las clases de equivalencia de $\mathscr{S}$. No obstante, una vez establecidas las leyes fundamentales, todas las demás propiedades se pueden obtener utilizando los elementos de Z mismos.

Ejemplo 5: Demostrar: Para todo $a, b, c \in Z$,

$$(a)\ a \cdot 0 = 0 \cdot a = 0 \qquad (b)\ a(-b) = -(ab) \qquad (c)\ a(b - c) = ab - ac$$

$$(a) \qquad a + 0 = a \qquad (\mathbf{A}_5)$$

$$\text{Entonces,} \qquad a \cdot a + 0 = a \cdot a = a(a + 0) = a \cdot a + a \cdot 0 \qquad (\mathbf{D}_1)$$

$$\text{y} \qquad 0 = a \cdot 0 \qquad (\mathbf{A}_4)$$

Ahora bien, por $\mathbf{M}_2$, $0 \cdot a = a \cdot 0 = 0$ como se requiere. Pero, por razones que solo se aclararán posteriormente, vamos a demostrar que

$$0 \cdot a = a \cdot 0$$

sin apelar a la ley conmutativa de la multiplicación. Se tiene

$$a \cdot a + 0 = a \cdot a = (a+0)a = a \cdot a + 0 \cdot a \qquad (\mathbf{D}_2)$$

por tanto, $0 = 0 \cdot a$

y $0 \cdot a = a \cdot 0$

(b) $$0 = a \cdot 0 = a[b + (-b)] = a \cdot b + a(-b) \qquad (\mathbf{D}_1)$$

así que $a(-b)$ es un simétrico aditivo de $a \cdot b$. Pero $-(a \cdot b)$ es también un simétrico aditivo de $a \cdot b$, luego

$$a(-b) = -(a \cdot b) \qquad \text{(Teorema IV, Capítulo 2)}$$

(c) $$a(b-c) = a[b + (-c)] = ab + a(-c) \qquad (\mathbf{D}_1)$$
$$= ab + (-ac) \qquad \text{((b) arriba)}$$
$$= ab - ac$$

Nota: En (c) se ha remplazado $a \cdot b$ y $-(a \cdot c)$ por las formas más corrientes ab y $-ac$, respectivamente.

MULTIPLES Y POTENCIAS

La sección que tiene este nombre en el Capítulo 3 (página 33), se puede repetir cambiando N por Z^+.

Es de notar que, para el caso $S = Z$, podemos ahora identificar ka con $k \cdot a$. Además, como Z contiene el simétrico aditivo de cada uno de sus elementos, se verifican (ix)-(xi), pero no (ix)'-(xi)' para cualesquiera $m, n \in Z$. Lo cual es ciertamente trivial, pues cuando $a, b, m, n \in Z$, las propiedades (ix) y (xi) son entonces las leyes distributivas.

Problemas resueltos

1. Demostrar que $\sim$ sobre L es una relación de equivalencia.

Sean $(s, m), (t, n), (u, p) \in L$. Se tiene

(a) $(s, m) \sim (s, m)$ pues $s + m = s + m$; $\sim$ es reflexiva.

(b) Si $(s, m) \sim (t, n)$, es $(t, n) \sim (s, m)$ pues las dos exigen $s + n = t + m$; $\sim$ es simétrica.

(c) Si $(s, m) \sim (t, n)$ y $(t, n) \sim (u, p)$, es $s + n = t + m$, $t + p = u + n$, y $s + n + t + p = t + m + u + n$. Por A_4 del Capítulo 3, página 30, la última igualdad se puede remplazar por $s + p = m + n$; así que $(s, m) \sim (u, p)$ y $\sim$ es transitiva.

Con lo que, $\sim$, por ser reflexiva, simétrica y transitiva es una relación de equivalencia.

2. Si $s, m, p, r \in N$, demostrar

(a) $[(r+p), p] = [r^*, 1]$ (c) $[s, m] \cdot [r, r] = [r, r]$ (e) $[s, m] \cdot [r^*, r] = [s, m]$

(b) $[s, m] + [r, r] = [s, m]$ (d) $[s, m] + [m, s] = [r, r]$

(a) $\big((r+p), p\big) \sim (r^*, 1)$ pues $r + p + 1 = r^* + p$.
Luego $[(r+p), p] = [r^*, 1]$ como se afirmaba.

(b) $[s, m] + [r, r] = [(s+r), (m+r)]$. Pero $\big((s+r), (m+r)\big) \sim (s, m)$ pues $(s+r) + m = s + (m+r)$.
Luego $[(s+r), (m+r)] = [s, m] + [r, r] = [s, m]$.

(c) $[s, m] \cdot [r, r] = [(s \cdot r + m \cdot r), (s \cdot r + m \cdot r)] = [r, r]$ pues $s \cdot r + m \cdot r + r = s \cdot r + m \cdot r + r$.

(d) $[s, m] + [m, s] = [(s+m), (s+m)] = [r, r]$

(e) $[s, m] \cdot [r^*, r] = [(s \cdot r^* + m \cdot r), (s \cdot r + m \cdot r^*)] = [s, m]$ pues $s \cdot r^* + m \cdot r + m = s + s \cdot r + m \cdot r^* = s \cdot r^* + m \cdot r^*$.

3. Demostrar: La clase de equivalencia a que pertenece la suma (producto) de dos elementos de sendas clases de equivalencia de $\mathscr{J}$ es independiente de los elementos elegidos.

Sean $[a,b] = [s,m]$ y $[c,d] = [t,n]$. Entonces $(a,b) \sim (s,m)$ y $(c,d) \sim (t,n)$ de modo que $a + m = s + b$ y $c + n = t + d$. Demostraremos:

(*a*) $[a,b] + [c,d] = [s,m] + [t,n]$, primera parte del teorema;

(*b*) $a \cdot c + b \cdot d + s \cdot n + m \cdot t = a \cdot d + b \cdot c + s \cdot t + m \cdot n$, un lema necesario;

(*c*) $[a,b] \cdot [c,d] = [s,m] \cdot [t,n]$, segunda parte del teorema.

(*a*) Como $a + m + c + n = s + b + t + d$,

$$(a+c) + (m+n) = (s+t) + (b+d)$$

$$\big((a+c),(b+d)\big) \sim \big((s+t),(m+n)\big)$$

$$[(a+c),(b+d)] = [(s+t),(m+n)]$$

y $$[a,b] + [c,d] = [s,m] + [t,n]$$

(*b*) Comenzamos por la igualdad evidente

$$(a+m)\cdot(c+t) + (s+b)\cdot(d+n) + (c+n)\cdot(a+s) + (d+t)\cdot(b+m)$$
$$= (s+b)\cdot(c+t) + (a+m)\cdot(d+n) + (d+t)\cdot(a+s) + (c+n)\cdot(b+m)$$

que se reduce a

$$2(a\cdot c + b\cdot d + s\cdot n + m\cdot t) + (a\cdot t + m\cdot c + s\cdot d + b\cdot n) + (s\cdot c + n\cdot a + b\cdot t + m\cdot d)$$
$$= 2(a\cdot d + b\cdot c + s\cdot t + m\cdot n) + (a\cdot t + m\cdot c + s\cdot d + b\cdot n) + (s\cdot c + n\cdot a + b\cdot t + m\cdot d)$$

y por las leyes de cancelación del Capítulo 3 a la identidad requerida.

(*c*) Por (*b*) tenemos

$$(a\cdot c + b\cdot d) + (s\cdot n + m\cdot t) = (s\cdot t + m\cdot n) + (a\cdot d + b\cdot c)$$

Entonces. $$\big((a\cdot c + b\cdot d),(a\cdot d + b\cdot c)\big) \sim \big((s\cdot t + m\cdot n),(s\cdot n + m\cdot t)\big)$$

$$[(a\cdot c + b\cdot d),(a\cdot d + b\cdot c)] = [(s\cdot t + m\cdot n),(s\cdot n + m\cdot t)]$$

y así, pues, $$[a,b]\cdot[c,d] = [s,m]\cdot[t,n]$$

4. Demostrar la ley asociativa para la adición:

$$([s,m] + [t,n]) + [u,p] = [s,m] + ([t,n] + [u,p])$$

para cualesquiera $[s,m],[t,n],[u,p] \in \mathscr{J}$.

Hallamos que

$$([s,m] + [t,n]) + [u,p] = [(s+t),(m+n)] + [u,p] = [(s+t+u),(m+n+p)]$$

y, por otra parte, $$[s,m] + ([t,n] + [u,p]) = [s,m] + [(t+u),(n+p)] = [(s+t+u),(m+n+p)]$$

y resulta la ley

5. Demostrar la ley distributiva $\mathbf{D}_2$:

$$([s,m] + [t,n])\cdot[u,p] = [s,m]\cdot[u,p] + [t,n]\cdot[u,p]$$

para cualesquiera $[s,m],[t,n],[u,p] \in \mathscr{J}$.

Tenemos

$$\begin{aligned}
([s,m] + [t,n])\cdot[u,p] &= [(s+t),(m+n)]\cdot[u,p] \\
&= \big[\big((s+t)\cdot u + (m+n)\cdot p\big),\ \big((s+t)\cdot p + (m+n)\cdot u\big)\big] \\
&= [(s\cdot u + t\cdot u + m\cdot p + u\cdot p),\ (s\cdot p + t\cdot p + m\cdot u + n\cdot u)] \\
&= \big[\big((s\cdot u + m\cdot p) + (t\cdot u + n\cdot p)\big),\ \big((s\cdot p + m\cdot u) + (t\cdot p + n\cdot u)\big)\big] \\
&= [(s\cdot u + m\cdot p),(s\cdot p + m\cdot u)] + [(t\cdot u + n\cdot p),(t\cdot p + n\cdot u)] \\
&= [s,m]\cdot[u,p] + [t,n]\cdot[u,p]
\end{aligned}$$

6. (*a*) Demostrar que $a + (-a) = 0$ para todo $a \in Z$.

Sea $a \leftrightarrow [s, m]$; entonces $-a \leftrightarrow [m, s]$.

$$a + (-a) \leftrightarrow [s, m] + [m, s] = [(s + m), (m + s)] = [r, r] \leftrightarrow 0$$

y $a + (-a) = 0$.

(*b*) Si $x + a = b$ con $a, b \in Z$, mostrar que $x = b + (-a)$.

Si $x = b + (-a)$, $x + a = (b + (-a)) + a = b + ((-a) + a) = b$; así que $x = b + (-a)$ es solución de la ecuación $x + a = b$. Supóngase que hay una segunda solución y. Entonces $y + a = b = x + a$ y por A_4, $y = x$. Luego la solución es única.

7. Si $a, b \in Z$, demostrar: (1) $(-a) + (-b) = -(a + b)$, (2) $(-a) \cdot (-b) = a \cdot b$.

Sea $a \leftrightarrow [s, m]$ y $b \leftrightarrow [t, n]$; entonces $-a \leftrightarrow [m, s]$ y $-b \leftrightarrow [n, t]$.

(1), $(-a) + (-b) \leftrightarrow [m, s] + [n, t] = [(m + n), (s + t)]$

y $a + b \leftrightarrow [s, m] + [t, n] = [(s + t), (m + n)]$

De otro lado $-(a + b) \leftrightarrow [(m + n), (s + t)] \leftrightarrow (-a) + (-b)$

y $(-a) + (-b) = -(a + b)$

(2) $(-a) \cdot (-b) \leftrightarrow [m, s] \cdot [n, t] = [(m \cdot n + s \cdot t), (m \cdot t + s \cdot n)]$

y $a \cdot b \leftrightarrow [s, m] \cdot [t, n] = [(s \cdot t + m \cdot n), (s \cdot n + m \cdot t)]$

Pero $[(m \cdot n + s \cdot t), (m \cdot t + s \cdot n)] = [(s \cdot t + m \cdot n), (s \cdot n + m \cdot t)]$

y $(-a) \cdot (-b) = a \cdot b$

8. Demostrar la ley de tricotomía. Para cualesquiera $a, b \in Z$ una, y solo una, de las relaciones

$$(a)\ a = b, \quad (b)\ a < b, \quad (c)\ a > b$$

es cierta.

Sean $a \leftrightarrow [s, m]$ y $b \leftrightarrow [t, n]$; entonces, por la ley de tricotomía del Capítulo 3, página 32, es cierta una, y solo una, de las (*a*) $s + n = t + m$ y $a = b$, (*b*) $s + n < t + m$ y $a < b$, (*c*) $s + n > t + m$ y $a > b$.

9. Si $a, b, c \in Z$, demostrar: $a + c > b + c$ si, y solo si, $a > b$.

Tomando $a \leftrightarrow [s, m]$, $b \leftrightarrow [t, n]$ y $c \leftrightarrow [u, p]$. Supóngase, ante todo, que

$$a + c > b + c \quad \text{o bien} \quad ([s, m] + [u, p]) > ([t, n] + [u, p])$$

Pero esto implica $[(s + u), (m + p)] > [(t + u), (n + p)]$

lo que, a su vez, implica $(s + u) + (n + p) > (t + u) + (m + p)$

Así que por el Teorema 11', Capítulo 3, página 33, $(s + n) > (t + m)$ o $[s, m] > [t, n]$ y $a > b$, como se afirmaba.

Supóngase ahora que $a > b$ o bien $[s, m] > [t, n]$; entonces, $(s + n) > (t + m)$. Para comparar ahora

$$a + c \leftrightarrow [(s + u), (m + p)] \quad \text{y} \quad b + c \leftrightarrow [(t + u), (n + p)]$$

se comparan $[(s + u), (m + p)]$ y $[(t + u), (n + p)]$

o bien $(s + u) + (n + p)$ y $(t + u) + (m + p)$

o bien $(s + n) + (u + p)$ y $(t + m) + (u + p)$

Como $(s+n) > (t+m)$, se sigue el Teorema II', Capitulo 3, página 33, que

$$(s+n) + (u+p) > (t+m) + (u+p)$$

Entonces, $$(s+u) + (n+p) > (t+u) + (m+p)$$

$$[(s+u),(m+p)] > [(t+u),(n+p)]$$

y $$a + c > b + c$$

como se afirmaba.

10. Si $a, b, c \in Z$, demostrar: Si $c < 0$, es $a \cdot c < b \cdot c$ si, y solo si, $a > b$.

Tómese $a \leftrightarrow [s, m]$, $b \leftrightarrow [t, n]$ y $c \leftrightarrow [u, p]$, en donde $u < p$, ya que $c < 0$.

(*a*) Supóngase $a \cdot c < b \cdot c$; entonces

$$[(s \cdot u + m \cdot p), (s \cdot p + m \cdot u)] < [(t \cdot u + n \cdot p), (t \cdot p + n \cdot u)]$$

y $$(s \cdot u + m \cdot p) + (t \cdot p + n \cdot u) < (t \cdot u + n \cdot p) + (s \cdot p + m \cdot u)$$

Como $u < p$, existe un $k \in N$ tal que $u + k = p$. Remplazando, pues, p en la desigualdad anterior, se tiene

$$(s \cdot u + m \cdot u + m \cdot k + t \cdot u + t \cdot k + n \cdot u) < (t \cdot u + n \cdot u + n \cdot k + s \cdot u + s \cdot k + m \cdot u)$$

de donde $$m \cdot k + t \cdot k < n \cdot k + s \cdot k$$

Así, pues, $$(m+t) \cdot k < (n+s) \cdot k$$

$$m + t < n + s$$

$$s + n > t + m$$

y $$a > b$$

(*b*) Supóngase $a > b$. Invirtiendo simplemente los pasos en (*a*), se tiene $a \cdot c < b \cdot c$, según lo afirmado.

11. Demostrar: Si $a, b \in Z$ y $a \cdot b = 0$, entonces es $a = 0$, o bien $b = 0$.

Supóngase $a \neq 0$; entonces $a \cdot b = 0 = a \cdot 0$ y por $\mathbf{M}_4$, $b = 0$. Análogamente, si $b \neq 0$ es $a = 0$.

12. Demostrar: No existe ningún $n \in Z^+$, tal que $0 < n < 1$.

Supóngase lo contrario y sea $m \in Z^+$ el mínimo entero con tal propiedad. De $0 < m < 1$, se tiene por (2), página 41, $0 < m^2 < m < 1$. Ahora bien, $0 < m^2 < 1$ y $m^2 < m$ contradicen la hipótesis de que m es el mínimo, con lo que queda el teorema demostrado.

13. Demostrar: Si $a, b \in Z$, es $a < b$ si, y solo si, $a - b < 0$.

Sean $a \leftrightarrow [s, m]$ y $b \leftrightarrow [t, n]$. Entonces

$$a - b = a + (-b) \leftrightarrow [s, m] + [n, t] = [(s+n), (m+t)]$$

Si $a < b$, es $s + n < m + t$ y $a - b < 0$. Reciprocamente, si $a - b < 0$, es $s + n < m + t$ y $a < b$.

14. Demostrar: $|a + b| \leq |a| + |b|$ para cualesquiera $a, b \in Z$.

Supóngase $a > 0$ y $b > 0$; entonces $|a + b| = a + b = |a| + |b|$.

Supóngase $a < 0$ y $b < 0$; entonces $|a + b| = -(a + b) = -a + (-b) = |a| + |b|$.

Supóngase $a > 0$ y $b < 0$ de modo que $|a| = a$ y $|b| = -b$. Y ahora, o bien $a + b = 0$ y $|a + b| = 0 < |a| + |b|$ o bien

$$a + b < 0 \quad \text{y} \quad |a + b| = -(a + b) = -a + (-b) = -|a| + |b| < |a| + |b|$$

o bien $$a + b > 0 \quad \text{y} \quad |a + b| = a + b = a - (-b) = |a| - |b| < |a| + |b|$$

El caso $a < 0$ y $b > 0$ se deja como ejercicio.

15. Demostrar: $|a \cdot b| = |a| \cdot |b|$ para cualesquiera $a, b \in Z$.

Supóngase $a > 0$ y $b > 0$; entonces $|a| = a$ y $|b| = b$. Con lo que $|a \cdot b| = a \cdot b = |a| \cdot |b|$.
Supóngase $a < 0$ y $b < 0$; entonces $|a| = -a$ y $|b| = -b$. Como $a \cdot b > 0$, es $|a \cdot b| = a \cdot b = (-a) \cdot (-b) = |a| \cdot |b|$.

Supóngase $a > 0$ y $b < 0$; entonces $|a| = a$ y $|b| = -b$. Como $a \cdot b < 0$, $|a \cdot b| = -(a \cdot b) = a \cdot (-b) = |a| \cdot |b|$.

El caso $a < 0$ y $b > 0$ se deja como ejercicio.

16. Demostrar que si a y b son enteros tales que $a \cdot b = 1$, entonces a y b son ambos 1 o ambos -1.

Primero se ve que ni a ni b pueden ser cero. Ahora bien, $|a \cdot b| = |a| \cdot |b| = 1$ y por el Problema 12, $|a| \geq 1$ y $|b| \geq 1$. Si $|a| > 1$ (también si $|b| > 1$), $|a| \cdot |b| \neq 1$. Luego $|a| = |b| = 1$ y en vista del Problema 7(b), se sigue el teorema.

Problemas propuestos

17. Demostrar: Si $r, s \in N$,

(a) $(r, r) \sim (s, s) \sim (1, 1)$ (d) $(r^*, r) \neq (r, r^*)$

(b) $(r^*, r) \sim (s^*, s) \sim (2, 1)$ (e) $(r^*, r) \neq (s, s^*)$

(c) $(r, r^*) \sim (s, s^*) \sim (1, 2)$ (f) $(r^* \cdot s^* + 1,\ r^* + s^*) \sim \big((r \cdot s)^*,\ 1\big)$

18. Enunciar y demostrar: (a) la ley asociativa para la multiplicación, (b) la ley conmutativa para la adición, (c) la ley conmutativa para la multiplicación, (d) la ley de cancelación sobre $\mathscr{I}$.

19. Demostrar: $[r^*, r] \leftrightarrow 1$ y $[r, r^*] \leftrightarrow -1$.

20. Si $a \in Z$, demostrar: (a) $a \cdot 0 = 0 \cdot a = 0$, ($b$) $(-1) \cdot a = -a$, (c) $-0 = 0$.

21. Si $a, b \in Z$, demostrar: (a) $-(-a) = +a$, (b) $(-a)(-b) = a \cdot b$, (c) $(-a) + b = -(a + (-b))$.

22. Con $b \in Z^+$, mostrar que $a - b < a + b$ para todo $a \in Z$.

23. Con $a, b \in Z$, demostrar (1), (2), (2') y (3'), página 41, de las relaciones de orden.

24. Con $a, b, c \in Z$, demostrar $a \cdot (b - c) = a \cdot b - a \cdot c$.

25. Demostrar que si $a, b \in Z$ y $a < b$, existe entonces algún $c \in Z^+$ tal que $a + c = b$.

Sugerencia: Para a y b representados como en el Problema 7 tómese $c \leftrightarrow [(r + m), (n + s)]$.

26. Demostrar: Si $a, b, c, d \in Z$,

(*a*) $-a > -b$ si $a < b$.
(*b*) $a + c < b + d$ si $a < b$ y $c < d$.
(*c*) Si $a < (b + c)$, entonces $a - b < c$.
(*d*) $a - b = c - d$ si, y solo si, $a + d = b + c$.

27. Demostrar que las relaciones de orden son bien definidas.

28. Demostrar la ley de cancelación para la multiplicación.

29. Definir sumas y productos de $n > 2$ elementos de Z y muéstrese que en tales sumas y productos se pueden intercalar paréntesis a voluntad.

30. Demostrar: (*a*) $m^2 > 0$ para todo entero $m \neq 0$.
(*b*) $m^3 > 0$ para todo entero $m > 0$.
(*c*) $m^3 < 0$ para todo entero $m < 0$.

31. Demostrar sin utilizar clases de equivalencia (véase Ejemplo 5):

(*a*) $-(-a) = a$
(*b*) $(-a)(-b) = ab$
(*c*) $(b - c) = (b + a) - (c + a)$
(*d*) $a(b - c) = ab - ac$
(*e*) $(a + b)(c + d) = (ac + ad) + (bc + bd)$
(*f*) $(a + b)(c - d) = (ac + bc) - (ad + bd)$
(*g*) $(a - b)(c - d) = (ac + bd) - (ad + bc)$

Capítulo 5

Algunas propiedades de los enteros

DIVISORES

Un entero $a \neq 0$ se llama *divisor* (o *factor*) de un entero b (lo cual se escribe «$a \mid b$») si existe un entero c tal que $b = ac$. Cuando $a \mid b$ se dirá también que b es un *múltiplo entero* de a.

Ejemplo 1: (*a*) $2 \mid 6$ pues $6 = 2 \cdot 3$

(*b*) $-3 \mid 15$ pues $15 = (-3)(-5)$

(*c*) $a \mid 0$, para todo $a \in Z$, pues $0 = a \cdot 0$

Para demostrar la necesidad de la restricción $a \neq 0$, supóngase que $0 \mid b$. Si $b \neq 0$ se debe tener $b = 0 \cdot c$ para algún $c \in Z$, lo cual es imposible; mientras que si $b = 0$, se tendría $0 = 0 \cdot c$, que es cierto para *cualquier* $c \in Z$.

Dados $b,c;x,y \in Z$ el entero $bx + cy$ se dice una combinación *lineal* de b y c. En el Problema 1 se demuestra que:

Teorema I. Si $a \mid b$ y $a \mid c$ entonces $a \mid (bx + cy)$ para cualesquiera $x, y \in Z$.

Véanse también Problemas 2 y 3.

PRIMOS

Como $a \cdot 1 = (-a)(-1) = a$ para todo $a \in Z$, se sigue que ± 1 y $\pm a$ son divisores de a. Un entero $p \neq 0, \pm 1$, se dice *primo* si, y solamente si, sus únicos divisores son ± 1 y $\pm p$.

Ejemplo 2: (*a*) Los enteros 2 y -5 son primos, en tanto que $6 = 2 \cdot 3$ y $-39 = 3(-13)$ no son primos.

(*b*) Los primeros 10 primos positivos son 2, 3, 5, 7, 11, 13, 17, 19, 23, 29.

Es claro que $-p$ es primo si, y solamente si, p lo es. En lo sucesivo nos referiremos sobre todo a los primos positivos. En el Problema 4 se demuestra que:

El número de primos positivos es infinito.

Si $a = bc$ con $|b| > 1$ y $|c| > 1$, se dice que a es *compuesto*. Así, pues, todo entero $a \neq 0, \pm 1$ o es primo o es compuesto.

MAXIMO COMUN DIVISOR

Si $a \mid b$ y $a \mid c$ se dice que a es un *divisor común* de b y c. Si, además, todo divisor común de b y c es también divisor de a, se dice que a es el *máximo común divisor* de b y c.

Ejemplo 3: (*a*) $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$ son divisores comunes de 24 y 60.

(*b*) ± 12 son máximos comunes divisores de 24 y 60.

(*c*) Los máximos comunes divisores de $b = 0$ y $c \neq 0$ son $\pm c$.

Sean c y d dos máximos comunes divisores distintos de $a \neq 0$ y $b \neq 0$. Entonces $c \mid d$ y $d \mid c$; luego, por el Problema 3, c y d difieren solamente en signo. Por comodidad, en lo que sigue limitaremos nuestra atención al máximo común divisor positivo de dos enteros a y b y utilizaremos d o bien (a, b) para designarlo. Así, pues, d es ciertamente el entero más grande (máximo) que divide a ambos a y b.

Ejemplo 4: Un procedimiento familiar para encontrar (210, 510) consiste en expresar cada entero como producto de sus factores primos, esto es, $210 = 2 \cdot 3 \cdot 5 \cdot 7$, $510 = 2 \cdot 3 \cdot 5 \cdot 17$, y formar el producto $2 \cdot 3 \cdot 5 = 30$ de sus factores comunes.

En el Ejemplo 4 hemos supuesto tácticamente (*a*) que todo par de enteros no nulos tienen un máximo común divisor positivo, y (*b*) que todo entero $a > 1$ tiene una factorización única, excepto en el orden de los factores, como producto de primos positivos. Desde luego, en (*b*) debe entenderse que, cuando a es primo, «un producto de primos positivos» consiste de un solo primo. Después se demostrarán estas proposiciones. Por el momento vamos a exponer otra manera de hallar el máximo común divisor de dos enteros no nulos. Empezamos con el

Algoritmo de la división. Para cualesquiera enteros no nulos a y b existen enteros únicos q y r llamados, respectivamente, *cociente* y *residuo*, tales que

$$a = bq + r, \quad 0 \leq r < |b| \tag{1}$$

Para una demostración, véase Problema 5.

Ejemplo 5:
(*a*) $780 = -48(-16) + 12$ (*c*) $826 = 25 \cdot 33 + 1$
(*b*) $-2805 = 119(-24) + 51$ (*d*) $758 = 242(3) + 32$

De (*1*) se sigue que $b \mid a$ y $(a, b) = b$ si, y solamente si, $r = 0$. Si $r \neq 0$, es fácil demostrar que un divisor común de a y b divide también a r y que un divisor común de b y r divide también a a. Entonces $(a, b) \mid (b, r)$ y $(b, r) \mid (a, b)$ de modo que, por el Problema 3, $(a, b) = (b, r)$. Ahora bien, o $r \mid b$ (véanse Ejemplos 5(*a*) y 5(*c*)) o $r \mid b$ (véanse Ejemplos 5(*b*) y 5(*d*)). En este caso, empleando el algoritmo de la división, se tiene

$$b = rq_1 + r_1, \quad 0 < r_1 < r \tag{2}$$

Y nuevamente, o bien $r_1 \mid r$ y $(a, b) = r_1$ o, empleando el algoritmo de la división,

$$r = r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \tag{3}$$

y $\quad (a, b) = (b, r) = (r, r_1) = (r_1, r_2)$.

Como los residuos $r_1, r_2, \ldots$, suponiendo que el proceso se continúe, constituyen un conjunto de enteros decrecientes no negativos, debe haber alguno nulo. Supóngase que el proceso termina con

$$(k) \qquad r_{k-3} = r_{k-2} \cdot q_{k-1} + r_{k-1} \qquad 0 < r_{k-1} < r_{k-2}$$
$$(k+1) \qquad r_{k-2} = r_{k-1} \cdot q_k + r_k \qquad 0 < r_k < r_{k-1}$$
$$(k+2) \qquad r_{k-1} = r_k \cdot q_{k+1} + 0$$

Entonces $(a, b) = (b, r) = (r, r_1) = \cdots = (r_{k-2}, r_{k-1}) = (r_{k-1}, r_k) = r_k$.

Ejemplo 6:

(*a*) En el Ejemplo 5(*b*), $51 \nmid 119$. Procediendo como en (*2*), hallamos que $119 = 51(2) + 17$. Como $17 \mid 51$: luego, $(-2805, 119) = 17$.

(*b*) En el Ejemplo 5(*d*), $32 \nmid 242$. De las igualdades sucesivas

$$\begin{aligned} 758 &= 242(3) + 32 \\ 242 &= 32(7) + 18 \\ 32 &= 18(1) + 14 \\ 18 &= 14(1) + 4 \\ 14 &= 4(3) + 2 \\ 4 &= 2(2) \end{aligned}$$

se concluye que $(758, 242) = 2$.

Despejando ahora en (1) $r = a - bq = a + (-q)b = m_1 a + n_1 b$; y

sustituyendo en (2) $r_1 = b - rq_1 = b - (m_1 a + n_1 b)q_1$
$= -m_1 q_1 a + (1 - n_1 q_1)b = m_2 a + n_2 b$

sustituyendo en (3) $r_2 = r - r_1 q_2 = (m_1 a + n_1 b) - (m_2 a + n_2 b)q_2$
$= (m_1 - q_2 m_2)a + (n_1 - q_2 n_2)b = m_3 a + n_3 b$

y siguiendo así se obtiene finalmente

$$r_k = m_{k+1} a + n_{k+1} b$$

Así, pues, tenemos

Teorema II. Si $d = (a, b)$ existen $m, n \in Z$ tales que $d = (a, b) = ma + nb$.

Ejemplo 7: Hallar (726, 275) y expresarlo en la forma del Teorema II.

De	Se obtiene
$726 = 275 \cdot 2 + 176$	$11 = 77 - 22 \cdot 3 = 77 - (99 - 77) \cdot 3$
$275 = 176 \cdot 1 + 99$	$= 77 \cdot 4 - 99 \cdot 3$
$176 = 99 \cdot 1 + 77$	$= (176 - 99) \cdot 4 - 99 \cdot 3$
$99 = 77 \cdot 1 + 22$	$= 176 \cdot 4 - 99 \cdot 7$
$77 = 22 \cdot 3 + 11$	$= 176 \cdot 4 - (275 - 176) \cdot 7$
$22 = 11 \cdot 2$	$= 176 \cdot 11 - 275 \cdot 7$
	$= (726 - 275 \cdot 2) \cdot 11 - 275 \cdot 7$
	$= 11 \cdot 726 + (-29) \cdot 275$

Así, pues, $m = 11$ y $n = -29$.

Nota 1. El procedimiento para obtener m y n aquí es una alternativa del que se usó para obtener el Teorema II.

Nota 2. En $(a, b) = ma + nb$ los enteros m y n no son únicos; en realidad, $(a, b) = (m + kb)a - (n - ka)b$ para todo $k \in N$.

Véase Problema 6.

La importancia del Teorema II se ve en el

Ejemplo 8: Demostrar: Si $a \mid c$, si $b \mid c$ y si $(a, b) = d$, entonces $ab \mid cd$.

Como $a \mid c$ y $b \mid c$ existen entonces enteros s y t tales que $c = as = bt$. Por el Teorema II existen $m, n \in Z$ tales que $d = ma + nb$. Entonces

$$cd = cma + cnb = btma + asnb = ab(tm + sn)$$

y $ab \mid cd$.

Una segunda consecuencia del algoritmo de la división es el

Teorema III. Cualquier conjunto no vacío K de enteros cerrado con respecto a las operaciones binarias de adición y sustracción o bien es $\{0\}$ o consiste en todos los múltiplos de su mínimo elemento positivo.

He aquí un esquema de la demostración cuando $K \neq \{0\}$. Supóngase que K contiene el entero $a \neq 0$. Como K es cerrado con respecto a la adición y la sustracción, se tiene:

$a - a = 0 \in K$.
$0 - a = -a \in K$.
K contiene por lo menos un entero positivo.
K contiene un positivo entero mínimo, sea e.
Por inducción sobre n, K contiene todos los múltiplos positivos ne de e (demuéstrese).
K contiene todos los múltiplos enteros me de e.
Si $b \in K$, entonces $b = q \cdot e + r$ donde $0 \leq r < e$; luego $r = 0$ y entonces todo elemento de K es un múltiplo entero de e.

ENTEROS PRIMOS RELATIVOS

Para $a, b \in Z$ dados, supóngase que existen $m, n \in Z$ tales que $am + bn = 1$. Ahora bien, todo factor común de a y b es factor del segundo miembro 1; luego $(a, b) = 1$. Dos enteros a y b para los cuales $(a, b) = 1$ se dicen *primos relativos*.

Véase Problema 7.

En el Problema 8 se demuestra el

Teoremas IV. Si $(a, s) = (b, s) = 1$, entonces $(ab, s) = 1$.

FACTORES PRIMOS

En el Problema 9 se demuestra el

Teorema V. Si p es primo y si $p \mid ab$ donde $a, b \in Z$, entonces $p \mid a$ o bien $p \mid b$.

Aplicando reiteradamente el Teorema V, se tiene el

Teorema V'. Si p es primo y si p es divisor del producto $a \cdot b \cdot c \cdot \ldots \cdot t$ de n enteros, entonces p es divisor de uno al menos de estos enteros.

En el Problema 10 se demuestra

El teorema de factorización única. Todo entero $a > 1$ tiene una factorización única salvo en el orden,

$$(a) \qquad a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$$

en un producto de primos positivos.

Evidentemente, si (a) da la factorización de a, entonces

$$-a = -(p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n)$$

Además, como los p de (a) no son necesariamente distintos, podemos escribir

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_s^{\alpha_s}$$

donde cada $\alpha_i \geq 1$ y los primos $p_1, p_2, p_3, \ldots, p_s$ son distintos.

Ejemplo 9: Expresar cada uno de los números 2,241,756 y 8,566,074 como producto de primos positivos y averiguar su máximo común divisor.

$$2{,}241{,}756 = 2^2 \cdot 3^4 \cdot 11 \cdot 17 \cdot 37 \text{ y } 8{,}566{,}074 = 2 \cdot 3^4 \cdot 11^2 \cdot 19 \cdot 23$$

Su máximo común divisor es $2 \cdot 3^4 \cdot 11$.

CONGRUENCIAS

Sea m un número positivo. La relación *congruente módulo* m ($\equiv \pmod m$) se define para todos los pares $a, b \in Z$ por $a \equiv b \pmod m$ si, y solamente si, $m \mid (a - b)$.

Ejemplo 10:

(a) $89 \equiv 25 \pmod 4$ porque $4 \mid (89 - 25) = 64$

(b) $89 \equiv 1 \pmod 4$ porque $4 \mid 88$

(c) $25 \equiv 1 \pmod 4$ porque $4 \mid 24$

(d) $153 \equiv -7 \pmod 8$ porque $8 \mid 160$

(e) $24 \not\equiv 3 \pmod 5$ porque $5 \nmid 21$

(f) $243 \not\equiv 167 \pmod 7$ porque $7 \nmid 76$

(g) Todo entero a es congruente módulo m con el resto de la división de a por m.

Otra definición, más útil con frecuencia que la original, es $a \equiv b \pmod m$ si, y solamente si, a y b dejan el mismo residuo al ser divididos por m.

Como consecuencias inmediatas de estas definiciones tenemos:

Teorema VI. Si $a \equiv b \pmod m$, entonces, para todo $n \in Z$, $mn + a \equiv b \pmod m$ y reciprocamente.

Teorema VII. Si $a \equiv b(\text{mod } m)$, es para todo $x \in Z$, $a + x \equiv b + x(\text{mod } m)$ y $ax \equiv bx(\text{mod } m)$.

Teorema VIII. Si $a \equiv b(\text{mod } m)$ y $c \equiv e(\text{mod } m)$, es $a + c \equiv b + e(\text{mod } m)$, $a - c \equiv b - e(\text{mod } m)$, $ac \equiv be(\text{mod } m)$.

Véase Problema 11.

Teorema IX. Sea $(c, m) = d$ y escríbase $m = m_1 d$. Si $ca \equiv cb(\text{mod } m)$ es entonces $a \equiv b(\text{mod } m_1)$ y recíprocamente.

Para una demostración, véase Problema 12.

Como caso especial del Teorema IX tenemos

Teorema X. Sea $(c, m) = 1$. Si $ca \equiv cb(\text{mod } m)$, entonces es $a \equiv b(\text{mod } m)$ y recíprocamente.

La relación $\equiv (\text{mod } m)$ sobre Z es una relación de equivalencia e induce una partición de los enteros en m clases de equivalencia, $[0], [1], [2], \ldots, [m-1]$, que se llaman *clases residuales módulo m*, siendo

$$[r] = \{a : a \in Z, a \equiv r(\text{mod } m)\}$$

Ejemplo 11: Las clases residuales módulo 4 son:

$$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$$
$$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$
$$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$$
$$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$$

Denotaremos el conjunto de todas las clases residuales módulo m por $Z/(m)$. Por ejemplo, $Z/(4) = \{[0], [1], [2], [3]\}$ y $Z/(m) = \{[0], [1], [2], [3], \ldots, [m-1]\}$. Es claro que $[3] \in Z/(4) = [3] \in Z/(m)$ si, y solamente si, $m = 4$. Dos propiedades fundamentales de las clases residuales módulo m son:

Si a y b son elementos de la misma clase residual $[s]$, entonces $a \equiv b(\text{mod } m)$.

Si $[s]$ y $[t]$ son clases residuales distintas con $a \in [s]$ y $b \in [t]$, es $a \not\equiv b(\text{mod } m)$.

EL ALGEBRA DE LAS CLASES RESIDUALES

Sean «$\oplus$» (adición) y «$\odot$» (multiplicación) definidas entre los elementos de $Z/(m)$ de la manera siguiente:

$$[a] \oplus [b] = [a + b]$$
$$[a] \odot [b] = [a \cdot b]$$

para toda $[a], [b] \in Z/(m)$.

Como $\oplus$ y $\odot$ sobre $Z/(m)$ se han definido respectivamente por $+$ y $\cdot$ sobre Z, se sigue inmediatamente que $\oplus$ y $\odot$ siguen las leyes $\mathbf{A_1}$-$\mathbf{A_4}$, $\mathbf{M_1}$-$\mathbf{M_4}$ y $\mathbf{D_1}$-$\mathbf{D_2}$ según la modificación del Capítulo 4, página 42.

Ejemplo 12: Las tablas suma y multiplicación para $Z/(4)$ son:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla 5-1

y

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabla 5-2

donde, por comodidad, [0], [1], [2], [3] se han remplazado por 0, 1, 2, 3.

CONGRUENCIAS LINEALES

Examínese la *congruencia lineal*

$$(b) \qquad ax \equiv b(\text{mod } m)$$

en donde a, b, m son enteros dados con $m > 0$. Se dice *solución* de la congruencia un entero $x = x_1$ tal que $m \mid (ax_1 - b)$. Pero si x_1 es una solución de (b) tal que $m \mid (ax_1 - b)$, entonces para cualquier $k \in Z$, $m \mid (a(x_1 + km) - b)$ y $x_1 + km$ es otra solución. Así, pues, si x_1 es una solución también lo es cualquier otro elemento de la clase residual $[x_1]$ módulo m. Si la congruencia lineal (b) tiene, pues, soluciones, éstas son los elementos de una o más clases residuales de $Z/(m)$.

Ejemplo 13:

(*a*) La congruencia $2x \equiv 3(\text{mod } 4)$ carece de solución, pues ninguno de los $2 \cdot 0 - 3, 2 \cdot 1 - 3, 2 \cdot 2 - 3, 2 \cdot 3 - 3$ es divisible por 4.

(*b*) La congruencia $3 \equiv 2(\text{mod } 4)$ tiene la solución 6 y, por tanto, todos los elementos de $[2] \in Z/(4)$ son soluciones. No hay otras.

(*c*) La congruencia $6x \equiv 2(\text{mod } 4)$ tiene 1 y 3 como soluciones. Como $3 \not\equiv 1(\text{mod } 4)$, diremos que 1 y 3 son *soluciones incongruentes* de la congruencia. Desde luego, todos los elementos de $[1], [3] \in Z/(4)$ son soluciones y no hay otras.

Volviendo a (b) supóngase que $(a, m) = 1 = sa + tm$. Entonces $b = bsa + btm$ y $x_1 = bs$ es solución. Supóngase ahora que $x_2 \not\equiv x_1(\text{mod } m)$ sea otra solución. Como $ax_1 \equiv b(\text{mod } m)$ y $ax_2 \equiv b(\text{mod } m)$, se sigue de la propiedad transitiva de $\equiv (\text{mod } m)$ que $ax_1 \equiv ax_2(\text{mod } m)$. Entonces $m \mid a(x_1 - x_2)$ y $x_1 \equiv x_2(\text{mod } m)$ en contradicción con nuestra hipótesis. Así que (b) solo tiene una solución incongruente, x_1, y la clase residual $[x_1] \in Z/(m)$, también llamada *clase de congruencia*, contiene todas las soluciones.

Ahora supóngase que $(a, m) = d = sa + tm$, $d > 1$. Como $a = a_1 d$ y $m = m_1 d$ se sigue que si (b) tiene una solución $x = x_1$, entonces $ax_1 - b = mq = m_1 dq$ y que $d \mid b$. Recíprocamente, supóngase que $d = (a, m)$ es un divisor de b y escríbase $b = b_1 d$. Por el Teorema IX, página 53, toda solución de (b) es solución de

$$(c) \qquad a_1 x \equiv b_1(\text{mod } m_1)$$

y toda solución de (c) lo es de (b). Ahora bien, $(a_1, m_1) = 1$, de modo que (c) tiene una sola solución incongruente y, por tanto, (b) tiene soluciones. Hemos demostrado la primera parte del

Teorema XI. La congruencia $ax \equiv b(\text{mod } m)$ tiene solución si, y solo si, $d = (a, m)$ es un divisor de b. Si $d \mid b$, la congruencia tiene exactamente d soluciones incongruentes (d clases de congruencia de soluciones).

Para completar la demostración, sea el subconjunto

$$S = \{x_1, x_1 + m_1, x_1 + 2m_1, x_1 + 3m_1, \ldots, x_1 + (d-1)m_1\}$$

de $[x_1]$, la totalidad de las soluciones de $a_1 x \equiv b_1(\text{mod } m_1)$. Demostraremos ahora que no hay dos elementos de S congruentes módulo m (así, pues, (b) tiene por lo menos d soluciones incongruentes), en tanto que cada elemento de $[x_1] - S$ es congruente módulo m con algún elemento de S (así que (b) tiene a lo más d soluciones incongruentes).

Sean $x_1 + sm_1$ y $x_1 + tm_1$ elementos distintos de S. Ahora bien, si $x_1 + sm_1 \equiv x_1 + tm_1(\text{mod } m)$ entonces $m \mid (s - t)m_1$; luego $d \mid (s - t)$ y $s = t$ en contradicción con lo supuesto de que $s \neq t$. De modo que los elementos de S son incongruentes módulo m. Considérese ahora cualquier elemento de $[x_1] - S$, sea $x_1 + (qd + r)m_1$ donde $q \geq 1$ y $0 \leq r < d$. Se tiene $x_1 + (qd + r)m_1 = x_1 + rm_1 + qm \equiv x_1 + rm_1(\text{mod } m)$ y $x_1 + rm_1 \in S$. Así, pues, la congruencia (b), con $(a, m) = d$ y $d \mid b$, tiene exactamente d soluciones incongruentes.

Véase Problema 14.

NOTACION DE POSICION DE LOS ENTEROS

Ya es bien sabido que

$$827{,}016 \;=\; 8\cdot 10^5 + 2\cdot 10^4 + 7\cdot 10^3 + 0\cdot 10^2 + 1\cdot 10 + 6$$

Lo que no es más que una aplicación de las propiedades de congruencia de los enteros. Porque, supóngase que a es un entero positivo. Por el algoritmo de la división $a = 10\cdot q_0 + r_0$, $0 \le r_0 < 10$. Si $q_0 = 0$, se escribe $a = r_0$; si $q_0 > 0$, entonces $q_0 = 10\cdot q_1 + r_1$, $0 \le r_1 < 10$. Ahora bien, si $q_1 = 0$, entonces $a = 10\cdot r_1 + r_2$ y se escribe $a = r_1 r_0$; si $q_1 > 0$, entonces $q_1 = 10\cdot q_2 + r_2$, $0 \le r_2 < 10$. Y otra vez, si $q_2 = 0$, entonces $a = 10^2\cdot r_2 + 10\cdot r_1 + r_0$ y se escribe $a = r_2 r_1 r_0$; si $q_2 > 0$, se repite el proceso. Del hecho de que los q constituyen un conjunto de enteros no negativos decrecientes, se sigue que el proceso debe terminar y se tiene

$$a \;=\; 10^s\cdot r_s + 10^{s-1}\cdot r_{s-1} + \cdots + 10\cdot r_1 + r_0 \;=\; r_s r_{s-1}\cdots r_1 r_0$$

Nótese que en esta representación los símbolos r_i utilizados pertenecen al conjunto $\{0, 1, 2, 3, \ldots, 9\}$ de residuos módulo 10. (¿Por qué es única esta representación?)

En el párrafo anterior hemos escogido el entero particular 10, llamado base, porque nos lleva a nuestro sistema de representación; pero el proceso es independiente de la base y cualquier otro entero positivo se puede utilizar para ello. Así, tomando 4 como base, cualquier entero positivo vendrá representado por un guarismo con las cifras 0, 1, 2, 3. Por ejemplo, el entero que en base 10 es 155, es $155 = 4^3\cdot 2 + 4^2\cdot 1 + 4\cdot 2 + 3 = 2123$ (base 4).

La adición y la multiplicación se efectúan de la misma manera, no importa cuál sea la base; pero hay que utilizar tablas distintas para cada operación. Para la base 4 estas tablas son:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	10
2	2	3	10	11
3	3	10	11	12

Tabla 5-3

y

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	10	12
3	0	3	12	21

Tabla 5-4

Véase Problema 15.

Problemas resueltos

1. Demostrar que si $a \mid b$ y $a \mid c$, entonces $a \mid (bx + cy)$ donde $x, y \in Z$.

Como $a \mid b$ y $a \mid c$, hay enteros s, t tales que $b = as$ y $c = at$. Entonces $bx + cy = asx + aty = a(sx + ty)$ y $a \mid (bx + cy)$.

2. Demostrar: Si $a \mid b$ y $b \neq 0$, es $|b| \ge |a|$.

Como $a \mid b$ tenemos $b = ac$ para algún $c \in Z$. Entonces $|b| = |a|\cdot|c|$ con $|c| \ge 1$. Como $|c| \ge 1$, se sigue que $|a|\cdot|c| \ge |a|$, esto es $|b| \ge |a|$.

3. Demostrar que si $a \mid b$ y $b \mid a$, entonces $b = a$ o $b = -a$.

Como $a \mid b$ implica $a \neq 0$ y $b \mid a$ implica $b \neq 0$, se tiene $b = ac$ y $a = bd$ donde $c, d \in Z$. Ahora bien $a \cdot b = (bd)(ac) = abcd$ y, por la ley de cancelación, $1 = cd$. Entonces, por el Problema 16, Capítulo 4, $c = 1$ ó -1 y $b = ac = a$ o $-a$.

4. Demostrar: El número de primos positivos es infinito.

Supóngase lo contrario, es decir, que hay exactamente n primos positivos $p_1, p_2, p_3, \ldots, p_n$ escritos por orden de magnitud. Fórmese ahora el producto $a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$ y considérese el entero $a + 1$. Como ninguno de los p es divisor de $a + 1$, se sigue que $a + 1$ es un primo $> p_n$, o tiene un factor primo mayor que p_n, en contradicción con la hipótesis de que p_n es el mayor número primo. Así, pues, no hay ningún primo positivo máximo y su número es infinito.

5. Demostrar el algoritmo de la división: Para dos enteros no nulos a y b existen enteros únicos q y r tales que

$$a = bq + r, \qquad 0 \leq r < |b|$$

Defínase $S = \{a - bx: x \in Z\}$. Si $b < 0$, esto es, $b \leq -1$, entonces $b \cdot |a| \leq -|a| \leq a$ y $a - b \cdot |a| \geq 0$. Si $b > 0$, esto es $b \geq 1$, entonces $b \cdot (-|a|) \leq -|a| \leq a$ y $a - b(-|a|) \geq 0$. Así, pues, S contiene enteros no negativos; denótese con r el menor de éstos ($r \geq 0$) y supóngase $r = a - bq$. Ahora bien, si $r \geq |b|$ entonces $r - |b| \geq 0$ y $r - |b| = a - bq - |b| = a - (q + 1)b < r$ o $a - (q - 1)b < r$ contra nuestra elección de r como el menor entero no negativo $\in S$. Luego $r < |b|$.

Supóngase que hubiera otro par q', r' tal que

$$a = bq' + r', \qquad 0 \leq r' < |b|$$

entonces $bq' + r' = bq + r$ o sea $b(q' - q) = r - r'$ lo que implica $b \mid (r - r')$ y como $|r - r'| < |b|$, se tiene $r - r' = 0$; entonces $q' - q = 0$ porque $b \neq 0$. Así que $r' = r$, $q' = q$ y q y r son únicos.

6. Encontrar (389, 167) y expresarlo en la forma $389m + 167n$.

De	Se obtiene
$389 = 167 \cdot 2 + 55$	$1 = 55 - 2 \cdot 27$
$167 = 55 \cdot 3 + 2$	$= 55 \cdot 82 - 167 \cdot 27$
$55 = 2 \cdot 27 + 1$	$= 389 \cdot 82 - 167 \cdot 191$
$2 = 1 \cdot 2$	

Así, pues, $(389,167) = 1 = 82 \cdot 389 + (-191)(167)$.

7. Demostrar: Si $c \mid ab$ y si $(a, c) = 1$, entonces $c \mid b$.

De $1 = ma + nc$ resulta $b = mab + ncb$. Como c es divisor de $mab + ncb$, es divisor de b y $c \mid b$ como se pedía.

8. Demostrar: Si $(a, s) = (b, s) = 1$, es $(ab, s) = 1$.

Supóngase lo contrario, o sea que $(ab, s) = d > 1$ y sea $d = (ab, s) = mab + ns$. Entonces $d \mid ab$ y $d \mid s$. Como $(a, s) = 1$, se sigue que $d \nmid a$; luego, según el Problema 7, $d \mid b$. Pero esto contradice a $(b, s) = 1$; así que $(ab, s) = 1$.

9. Demostrar: Si p es primo y si $p \mid ab$, con $a, b \in Z$; entonces $p \mid a$ o bien $p \mid b$.

Si $p \mid a$ se tiene el teorema. Supóngase que $p \nmid a$. Por definición, los únicos divisores de p son ± 1 y $\pm p$; entonces $(p, a) = 1 = mp + na$ para ciertos $m, n \in Z$ por el Teorema II. Pero $b = mpb + nab$ y como $p \mid (mpb + nab)$, se sigue que $p \mid b$.

10. Demostrar: Todo entero $a > 1$ tiene una factorización única (salvo el orden de los factores) en producto de primos positivos.

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$$

Si a es primo, la representación es inmediata de acuerdo con el teorema. Si a es compuesto, considérese el conjunto $S = \{x: x > 1, x \mid a\}$. El elemento mínimo s de S no tiene más factores positivos que 1 y s; luego s es primo, llamémoslo p_1, y

$$a = p_1 \cdot b_1, \qquad b_1 > 1$$

Entonces, o bien b_1 es primo, digamos p_2, y $a = p_1 \cdot p_2$, o bien b_1, siendo compuesto, tiene un factor primo p_2 y

$$a = p_1 \cdot p_2 \cdot b_2, \qquad b_2 > 1$$

Reiterando el razonamiento se tiene $a = p_1 \cdot p_2 \cdot p_3$, o bien

$$a = p_1 \cdot p_2 \cdot p_3 \cdot b_3, \qquad b_3 > 1$$

y así sucesivamente.

Pero los elementos del conjunto $B = \{b_1, b_2, b_3, \ldots\}$ son tales que $b_1 > b_2 > b_3 \ldots$; luego B tiene elemento mínimo b_n que es primo, p_n y se tiene por último

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n$$

Para demostrar la unicidad, supóngase que hay dos representaciones

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_m$$

Ahora bien, q_1 es divisor de $p_1 \cdot p_2 \cdot p_3 \ldots p_n$; luego, por el Teorema V', q_1 es divisor de alguno de los factores p, digamos de p_1. Entonces, $q_1 = p_1$, ya que ambos son primos positivos y por M_4 del Capítulo IV.

$$p_2 \cdot p_3 \cdot \ldots \cdot p_n = q_2 \cdot q_3 \cdot \ldots \cdot q_m$$

Repitiendo este razonamiento las veces suficientes se encuentra que $m = n$ y que la factorización es única.

11. Hallar los menores enteros positivos módulo 5 con los cuales son congruentes 19, 288, $19 \cdot 288$ y $19^3 \cdot 288^2$.

Hallamos que

$19 = 5 \cdot 3 + 4$; luego $19 \equiv 4 \pmod 5$.

$288 = 5 \cdot 57 + 3$; luego $288 \equiv 3 \pmod 5$.

$19 \cdot 288 = 5(\cdots) + 12$; luego $19 \cdot 288 \equiv 2 \pmod 5$.

$19^3 \cdot 288^2 = 5(\cdots) + 4^3 \cdot 3^2 = 5(\cdots) + 576$; luego $19^3 \cdot 288^2 \equiv 1 \pmod 5$.

12. Demostrar: Sea $(c, m) = d$ y escríbase $m = m_1 d$. Si $ca \equiv cb \pmod m$, entonces $a \equiv b \pmod{m_1}$ y recíprocamente.

Escríbase $c = c_1 d$ de modo que $(c_1, m_1) = 1$. Si $m \mid c(a - b)$ esto es, si $m_1 d \mid c_1 d(a - b)$ entonces $m_1 \mid c_1(a - b)$ y, como $(c_1, m_1) = 1$, $m_1 \mid (a - b)$ y $a \equiv b \pmod{m_1}$.

Para la recíproca, supóngase que $a \equiv b \pmod{m_1}$. Como $m_1 \mid (a - b)$ se sigue que $m_1 \mid c_1(a - b)$ y $m_1 d \mid c_1 d(a - b)$. Así que $m \mid c(a - b)$ y $ca \equiv cb \pmod m$.

13. Demostrar que, si $a, b, p > 0 \in Z$, $(a + b)^p \equiv a^p + b^p \pmod p$.

Por el teorema del binomio $(a + b)^p = a^p + p(\ldots) + b^p$ y el teorema es inmediato.

14. Hallar las soluciones positivas mínimas incongruentes de

(a) $13x \equiv 9 \pmod{25}$ (c) $259x \equiv 5 \pmod{11}$ (e) $222x \equiv 12 \pmod{18}$

(b) $207x \equiv 6 \pmod{18}$ (d) $7x \equiv 5 \pmod{256}$

(a) Como $(13, 25) = 1$, la congruencia tiene, por el Teorema XI, una solución incongruente simple.

Solución I. Si x_1 es la solución, es claro entonces que x_1 es un entero cuya cifra de las unidades es 3 u 8; así, pues, $x_1 \in \{3, 8, 13, 18, 23\}$. Ensayando estos números, se encuentra que $x_1 = 18$.

Solución II. Por el proceso del máximo común divisor se encuentra $(13, 25) = 1 = -1 \cdot 25 + 2 \cdot 13$. Entonces, $9 = -9 \cdot 25 + 18 \cdot 13$ y 18 es la solución requerida.

(*b*) Como $207 = 18 \cdot 11 + 9$, $207 \equiv 9 \pmod{18}$, $207x \equiv 9x \pmod{18}$ y, por transitividad, la congruencia dada es equivalente a la $9x \equiv 6 \pmod{18}$. Por el Teorema IX, esta congruencia se puede reducir a $3x \equiv 2 \pmod 6$. Pero $(3, 6) = 3$ y $3 \nmid 2$; luego no hay solución.

(*c*) Como $259 = 11 \cdot 23 + 6$, $259 \equiv 6 \pmod{11}$ y la congruencia dada es equivalente a la $6x \equiv 5 \pmod{11}$. Esta congruencia tiene una sola solución incongruente que a simple vista es 10.

(*d*) Mediante el proceso del máximo común divisor se encuentra $(256, 7) = 1 = 2 \cdot 256 + 7(-73)$; así, pues, $5 = 10 \cdot 256 + 7(-365)$. Ahora bien, $-365 \equiv 147 \pmod{256}$ y la solución requerida es 147.

(*e*) Como $222 = 18 \cdot 12 + 6$, la congruencia dada es equivalente a la $6x \equiv 12 \pmod{18}$. Como $(6, 18) = 6$ y $6 \mid 12$, hay exactamente 6 soluciones incongruentes. Como se muestra en la demostración del Teorema XI, estas 6 soluciones son los primeros 6 enteros positivos en el conjunto de todas las soluciones de $x \equiv 2 \pmod 3$, es decir, los 6 primeros enteros positivos en $[2] \in Z/(\text{mod } 3)$. Son entonces 2, 5, 8, 11, 14, 17.

15. Escribir 141 y 152 en base 4. Hacer su suma y producto y comprobar los resultados.

$141 = 4^3 \cdot 2 + 4^2 \cdot 0 + 4 \cdot 3 + 1$; la representación es 2031.

$152 = 4^3 \cdot 2 + 4^2 \cdot 1 + 4 \cdot 2 + 0$; la representación es 2120.

Suma

$1 + 0 = 1$; $3 + 2 = 11$, se escribe 1 y se lleva 1; $1 + 1 + 0 = 2$; $2 + 2 = 10$

Así que la suma es 10211 en base 4 y 293 en base 10.

Producto

Multipliquese por 0:	0000
Multipliquese por 2: $2 \cdot 1 = 2$; $2 \cdot 3 = 12$, se escribe 2 y se lleva 1; etc.	10122
Multipliquese por 1:	2031
Multipliquese por 2:	10122
	11032320

El producto es 11032320 en base 4 y 21432 en base 10.

Problemas propuestos

16. Mostrar que la relación ($\mid$) es reflexiva y transitiva, pero no simétrica.

17. Demostrar que si $a \mid b$ entonces $-a \mid b$, $a \mid -b$ y $-a \mid -b$.

18. Enumerar todos los primos positivos (*a*) <50, (*b*) <200.
Resp. (*a*) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

19. Demostrar: Si $a = b \cdot q + r$ donde $a, b, q, r \in Z$, entonces todo divisor común de a y b divide también a r, y todo divisor común de b y r también divide a a.

20. Hallar el máximo común divisor de cada par de enteros y expresarlo en la forma del Teorema II:

(*a*) 237, 81 *Resp.* $3 = 13 \cdot 237 + (-38) \cdot 81$

(*b*) 616, 427 *Resp.* $7 = -9 \cdot 616 + 13 \cdot 427$

(*c*) 936, 666 *Resp.* $18 = 5 \cdot 936 + (-7) \cdot 666$

(*d*) 1137, 419 *Resp.* $1 = 206 \cdot 1137 + (-559) \cdot 419$

21. Demostrar: Si $s \neq 0$, entonces $(sa, sb) = |s| \cdot (a, b)$.

22. Demostrar: (*a*) Si $a \mid s$, $b \mid s$ y $(a, b) = 1$, entonces $ab \mid s$.
(*b*) Si $m = dm_1$ y si $m \mid am_1$, entonces $d \mid a$.

23. Demostrar: Si el primo p es divisor de $a \cdot b \cdot c$, entonces $p \mid a$ o $p \mid b$ o $p \mid c$.

24. El entero $e = [a, b]$ se llama *mínimo común múltiplo* de los enteros positivos a y b si (1) $a \mid e$ y $b \mid e$, (2) si $a \mid x$ y $b \mid x$, entonces $e \mid x$.

25. Hallar: (*a*) [3, 7], (*b*) [3, 12], (*c*) [22, 715]. *Resp.* (*a*) 21, (*b*) 12, (*c*) 1430

26. (*a*) Escribir los enteros $a = 19.500$ y $b = 54.450$ como productos de primos positivos.
(*b*) Hallar $d = (a, b)$ y $e = [a, b]$.
(*c*) Verificar $d \cdot e = a \cdot b$
(*d*) Demostrar la relación en (*c*) si a y b son enteros positivos cualesquiera.
Resp. (*b*) $2 \cdot 3 \cdot 5^2$; $2^2 \cdot 3^2 \cdot 5^3 \cdot 11^2 \cdot 13$

27. Demostrar: Si $m > 1$, $m \nmid a$, $m \nmid b$, entonces $m \mid (a - b)$ implica $a - mq_1 = r = b - mq_2$, $0 < r < m$, y recíprocamente.

28. Hallar todas las soluciones de:

(*a*) $4x \equiv 3 \pmod 7$ (*e*) $153x \equiv 6 \pmod{12}$
(*b*) $9x \equiv 11 \pmod{26}$ (*f*) $x + 1 \equiv 3 \pmod 7$
(*c*) $3x + 1 \equiv 4 \pmod 5$ (*g*) $8x \equiv 6 \pmod{422}$
(*d*) $8x \equiv 6 \pmod{14}$ (*h*) $363x \equiv 345 \pmod{624}$

Resp. (*a*) [6], (*b*) [7], (*c*) [1], (*d*) [6], [13], (*e*) [2], [6], [10], (*f*) [2], (*g*) [159], [370], (*h*) [123], [331], [539]

29. Demostrar: Teoremas V, VI, VII, VIII.

30. Demostrar: Si $a \equiv b \pmod m$ y $c \equiv b \pmod m$, entonces $a \equiv c \pmod m$. Véanse Ejemplos 10(*a*), (*b*), (*c*), página 52.

31. (*a*) Demostrar: Si $a + x \equiv b + x \pmod m$, es $a \equiv b \pmod m$.
(*b*) Dar un contraejemplo numérico como prueba en contrario de: Si $ax \equiv bx \pmod m$, entonces $ax \equiv b \pmod m$.
(*c*) Modifíquese este establecimiento falso de (*b*) para obtener uno verdadero.

32. (*a*) Interprétese $a \equiv b \pmod 0$.
(*b*) Muéstrese que todo $x \in Z$ es solución de $ax \equiv b \pmod 1$.

33. (*a*) Construir las tablas de adición y multiplicación para $Z/(5)$.
(*b*) Mediante la tabla de multiplicación obtener $3^2 \equiv 4 \pmod 5$, $3^4 \equiv 1 \pmod 5$, $3^8 \equiv 1 \pmod 5$.
(*c*) Obtener $3^{256} \equiv 1 \pmod 5$, $3^{514} \equiv 4 \pmod 5$, $3^{1024} \equiv 1 \pmod 5$.

34. Construir tablas de adición y multiplicación para $Z/(2)$, $Z/(6)$, $Z/(7)$, $Z/(9)$.

35. Demostrar: Si $[s] \in Z/(m)$ y si $a, b \in [s]$, entonces $a \equiv b \pmod m$.

36. Demostrar: Si $[s], [t] \in Z/(m)$ y si $a \in [s]$ y $b \in [t]$, entonces $a \equiv b \pmod m$ si, y solo si, $[s] = [t]$.

37. Expresar 212 en las bases (*a*) 2, (*b*) 3, (*c*) 4, (*d*) 7 y (*e*) 9.
Resp. (*a*) 11010100, (*b*) 21212, (*c*) 3110, (*d*) 422, (*e*) 255

38. Expresar 89 y 111 en distintas bases, hacer la suma y el producto y comprobar los resultados.

39. Demostrar la primera parte del teorema de factorización única utilizando el principio de inducción establecido en el Problema 27, Capítulo 3, página 37.

Capítulo 6

Los números racionales

LOS NUMEROS RACIONALES

El sistema de los enteros tiene un defecto manifiesto en que, dados dos enteros $m \neq 0$ y s, la ecuación $mx = s$ puede o no tener solución. Por ejemplo, $3x = 6$ tiene la solución $x = 2$, pero la $4x = 6$ no tiene solución. Este defecto se remedia añadiendo a los enteros otros números (llamados comúnmente fracciones) para formar el sistema Q de los *números racionales*. La construcción dada aquí es en lo esencial la que se utilizó en el Capítulo 4.

Se parte del conjunto de pares ordenados

$$K = I \times (I - \{0\}) = \{(s, m): s \in I, m \in I - \{0\}\}$$

y se define una relación binaria $\sim$ entre los (s, m), $(t, n) \in K$ por

$$(s, m) \sim (t, n) \quad \text{si, y solo si,} \quad sn = mt$$

(Obsérvese cuidadosamente que 0 puede aparecer como primer componente, pero *nunca* como segundo en cualquier (s, m).)

Pero entonces $\sim$ es una relación de equivalencia (probarlo) y así efectúa en K una partición en clases de equivalencia

$$\mathcal{J} = \{[s, m], [t, n], \ldots\}$$

donde $$[s, m] = \{(a, b): (a, b) \in K, (a, b) \sim (s, m)\}$$

Las clases de equivalencia de $\mathcal{J}$ se llamarán números racionales y en lo que sigue se verá que $\mathcal{J}$ es isomorfo al sistema Q tal como se le conoce.

ADICION Y MULTIPLICACION

La adición y la multiplicación sobre $\mathcal{J}$ se definen respectivamente por

(i) $$[s, m] + [t, n] = [(sn + mt), mn]$$

y

(ii) $$[s, m] \cdot [t, n] = [st, mn]$$

Estas operaciones así definidas en términos de operaciones bien definidas entre enteros son (véase Problema 1) bien definidas ellas mismas.

Definimos ahora dos números racionales especiales:

$$\textit{cero}: \ [0, m] \leftrightarrow 0 \qquad \textit{uno}: \ [m, m] \leftrightarrow 1$$

y los simétricos

(aditivo): $-[s, m] = [-s, m]$ para todo $[s, m] \in \mathcal{J}$

(multiplicativo): $[s, m]^{-1} = [m, s]$ para todo $[s, m] \in \mathcal{J}$ si $s \neq 0$.

En forma análoga a la del Capítulo 4, es fácil probar que la adición y la multiplicación siguen las leyes $\mathbf{A}_1$-$\mathbf{A}_6$, $\mathbf{M}_1$-$\mathbf{M}_5$, $\mathbf{D}_1$-$\mathbf{D}_2$, tales como se establecieron para los enteros.

Una propiedad de $\mathcal{J}$ pero no de Z es:

$\mathbf{M}_6$: Para todo $x \neq 0 \in \mathcal{J}$ existe un simétrico multiplicativo $x^{-1} \in \mathcal{J}$ tal que $x \cdot x^{-1} = x^{-1} \cdot x = 1$, que se llamā *inverso* de x.

Por el Teorema IV, Capítulo 2, el inverso definido en $\mathbf{M}_6$ es único.

En el Problema 2 se demuestra el

Teorema I. Si x y y son elementos no nulos de $\mathscr{I}$, entonces $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

SUSTRACCION Y DIVISION

La sustracción y la división sobre $\mathscr{I}$ se definen por

(iii) $x - y = x + (-y)$ para cualesquiera $x, y \in \mathscr{I}$

y

(iv) $x : y = x \cdot y^{-1}$ para cualesquiera $x \in \mathscr{I}$, $y \neq 0 \in \mathscr{I}$

respectivamente.

Estas operaciones no son ni asociativas ni conmutativas (demuéstrese esto). Pero, lo mismo que en Z, la multiplicación es distributiva con respecto a la sustracción.

RACIONALES ENTEROS

La aplicación $[t, 1] \in \mathscr{I} \leftrightarrow t \in Z$

es un isomorfismo de un cierto subconjunto de $\mathscr{I}$ sobre el conjunto de los enteros. Se puede, pues, siempre que sea más cómodo, remplazar el subconjunto $\mathscr{I}^* = \{[t, 1] : [t, 1] \in \mathscr{I}\}$ por Z. Para completar la identificación de $\mathscr{I}$ con Q no hay más que remplazar

$$x \cdot y^{-1} \quad \text{por} \quad x/y$$

y, en particular, $[s, m]$ por s/m.

RELACION DE ORDEN

Un elemento $x \in Q$, es decir, $x \leftrightarrow [s, m] \in \mathscr{I}$, se llama *positivo* si, y solamente si, $s \cdot m > 0$. El subconjunto de todos los elementos positivos de Q se designa por Q^+ y el subconjunto correspondiente de $\mathscr{I}$ por $\mathscr{I}^+$. Análogamente, $[s, m]$ se llama *negativo* si, y solamente si, $s \cdot m < 0$. El subconjunto de todos los elementos negativos de Q se designará por Q^- y el subconjunto correspondiente de $\mathscr{I}$ por $\mathscr{I}^-$. Como por la ley de tricotomía del Capítulo 4, o es $s \cdot m > 0$, o es $s \cdot m < 0$, o es $s \cdot m = 0$, se sigue que cada elemento de $\mathscr{I}$ es positivo, o negativo, o nulo.

Las relaciones de orden $<$ y $>$ sobre Q se definen como sigue:

Para todo par de elementos $x, y \in Q$,

$$x < y \quad \text{si, y solo si,} \quad x - y < 0$$

$$x > y \quad \text{si, y solo si,} \quad x - y > 0$$

Estas relaciones son transitivas, pero no reflexivas ni simétricas.

Q también cumple la

Ley de tricotomía: Si $x, y \in Q$, se verifica una, y solo una, de las relaciones

$$(a) \quad x = y \qquad (b) \quad x < y \qquad (c) \quad x > y$$

REDUCCION A TERMINOS MINIMOS

Considérese cualquier $[s, m] \in \mathscr{I}$ con $s \neq 0$. Sea d el máximo común divisor (positivo) de s y m y escríbase $s = ds_1$, $m = dm_1$. Como $(s, m) \sim (s_1, m_1)$, se sigue que $[s, m] = [s_1, m_1]$, es decir, que $s/m = s_1/m_1$. Así que cualquier número racional $\neq 0$ se puede escribir de manera única en la forma a/b donde a y b son primos relativos. Cuando s/m se remplaza por a/b se dice que s/m ha sido reducido a sus términos mínimos, con lo que ahora es irreducible. En lo sucesivo, todo número racional que intervenga en cualquier discusión se considerará como irreducible.

En el Problema 3 se demuestra:

Teorema II. Si x y y son racionales positivos con $x < y$, se sigue que $1/x > 1/y$.

En los Problemas 4 y 5 se demuestra:

Propiedad de densidad: Si x y y con $x < y$ son dos números racionales, existe un número racional z tal que $x < z < y$

y

Propiedad arquimediana: Si x y y son números racionales positivos existe un entero positivo p tal que $px > y$.

REPRESENTACION DECIMAL

Considérese el número racional positivo a/b con $b > 1$. Se tiene

$$a = q_0 b + r_0 \qquad 0 \leq r_0 < b$$

y

$$10r_0 = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

Como $r_0 < b$ y, por tanto, $q_1 b + r_1 = 10r_0 < 10b$, se sigue que $q_1 < 10$. Si $r_1 = 0$, entonces $r_0 = \frac{q_1}{10} b$, $a = q_0 b + \frac{q_1}{10} b$ y $\frac{a}{b} = q_0 + q_1/10$. Se escribe $a/b = q_0,q_1$ y se dice que q_0,q_1 es la representación decimal de a/b. Si $r_1 \neq 0$, se tiene

$$10r_1 = q_2 b + r_2 \qquad 0 \leq r_2 < b$$

en donde $q_2 < 10$. Si $r_2 = 0$, entonces $r_1 = \frac{q_2}{10} b$ de modo que $r_0 = \frac{q_1}{10} b + \frac{q_2}{10^2} b$ y la representación decimal de a/b es q_0,q_1q_2; si $r_2 = r_1$ la representación decimal de a/b es el número decimal periódico $q_0,q_1q_2q_2q_2\ldots$; si $r_2 \neq 0, r_1$, se repite el proceso.

Pero los distintos residuos $r_0, r_1, r_2, \ldots$, son elementos del conjunto $\{0, 1, 2, 3, \ldots, b-1\}$ de los residuos módulo b, de modo que, en el peor de los casos, r_b debe ser idéntico a alguno de los $r_0, r_1, r_2, \ldots, r_{b-1}$, digamos al r_c, y la representación decimal de a/b es el decimal periódico

$$q_0,q_1q_2q_3\ldots q_{b-1}q_{c+1}q_{c+2}\ldots q_{b-1}q_{c+1}q_{c+2}\ldots q_{b-1}\ldots$$

Así que todo número racional se puede expresar como un número decimal que termina o que es periódico.

Ejemplo 1: (a) $5/4 = 1{,}25$

(b) $3/8 = 0{,}375$

(c) Para 11/6 se encuentra

$$\begin{aligned} 11 &= 1\cdot 6 + 5; & q_0 &= 1, & r_0 &= 5 \\ 10\cdot 5 &= 8\cdot 6 + 2; & q_1 &= 8, & r_1 &= 2 \\ 10\cdot 2 &= 3\cdot 6 + 2; & q_2 &= 3, & r_2 &= 2 = r_1 \end{aligned}$$

y $\quad 11/6 = 1{,}833333\ldots$.

(d) Para 25/7 se encuentra

$$\begin{aligned} 25 &= 3\cdot 7 + 4; & q_0 &= 3, & r_0 &= 4 \\ 10\cdot 4 &= 5\cdot 7 + 5; & q_1 &= 5, & r_1 &= 5 \\ 10\cdot 5 &= 7\cdot 7 + 1; & q_2 &= 7, & r_2 &= 1 \\ 10\cdot 1 &= 1\cdot 7 + 3; & q_3 &= 1, & r_3 &= 3 \\ 10\cdot 3 &= 4\cdot 7 + 2; & q_4 &= 4, & r_4 &= 2 \\ 10\cdot 2 &= 2\cdot 7 + 6; & q_5 &= 2, & r_5 &= 6 \\ 10\cdot 6 &= 8\cdot 7 + 4; & q_6 &= 8, & r_6 &= 4 = r_0 \end{aligned}$$

y $\quad 25/7 = 3{,}571428\ 571428\ldots$.

Reciprocamente, claro está que todo decimal que termina es un número racional. Por ejemplo, $0{,}17 = 17/100$ y $0{,}175 = 175/1000 = 7/40$.

En el Problema 6 se demuestra el

Teorema III. Todo decimal periódico es un número racional.

La demostración emplea los dos teoremas preliminares:

(i) Todo decimal periódico se puede escribir como suma de una progresión geométrica infinita.

(ii) La suma de una progresión geométrica infinita cuya razón r es tal que $|r| < 1$, es un número finito.

En cualquier libro de álgebra que trate las progresiones se encuentra el estudio de estos teoremas.

Problemas resueltos

1. Demostrar que la adición y la multiplicación sobre $\mathscr{I}$ están bien definidas.

Sean $[a, b] = [s, m]$ y $[c, d] = [t, n]$. Entonces $(a, b) \sim (s, m)$ y $(c, d) \sim (t, n)$, de modo que $am = bs$ y $cn = dt$. Como

$$\begin{aligned} [a,b] + [c,d] &= [(ad+bc), bd] = [(ad+bc)mn, bd \cdot mn] \\ &= [(am \cdot dn + cn \cdot bm), bd \cdot mn] \\ &= [(bs \cdot dn + dt \cdot bm), bd \cdot mn] \\ &= [bd(sn+tm), bd \cdot mn] \\ &= [sn+tm, mn] = [s,m] + [t,n] \end{aligned}$$

y la adición es bien definida

Asimismo,
$$\begin{aligned} [a,b] \cdot [c,d] &= [ac, bd] = [ac \cdot mn, bd \cdot mn] \\ &= [am \cdot cn, bd \cdot mn] = [bs \cdot dt, bd \cdot mn] \\ &= [bd \cdot st, bd \cdot mn] = [st, mn] \\ &= [s,m] \cdot [t,n] \end{aligned}$$

y la multiplicación es bien definida

2. Demostrar: Si x, y son números racionales no nulos, entonces $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

Sean $x \leftrightarrow [s, m]$ y $y \leftrightarrow [t, n]$, de modo que $x^{-1} \leftrightarrow [m, s]$ y $y^{-1} \leftrightarrow [n, t]$. Entonces $x \cdot y \leftrightarrow [s, m] \cdot [t, n] = [st, mn]$ y $(x \cdot y)^{-1} \leftrightarrow [mn, st] = [n, t] \cdot [m, s] \leftrightarrow y^{-1} \cdot x^{-1}$.

3. Demostrar: Si x y y son racionales positivos con $x < y$, entonces $1/x > 1/y$.

Sean $x \leftrightarrow [s, m]$ y $y \leftrightarrow [t, n]$; entonces $sm > 0$, $tn > 0$, y $sn < mt$. Y así, para $1/x = x^{-1} \leftrightarrow [m, s]$ y $1/y \leftrightarrow [n, t]$, la desigualdad $mt > sn$ implica $1/x > 1/y$, como se afirmaba.

4. Demostrar: Si x y y con $x < y$ son dos números racionales, existe un número racional z tal que $x < z < y$.

Como $x < y$, tenemos

$$2x = x + x < x + y \quad \text{y} \quad x + y < y + y = 2y$$

Entonces
$$2x < x + y < 2y$$

y multiplicando por $\frac{1}{2}$, $x < \frac{1}{2}(x + y) < y$. Así, pues, $\frac{1}{2}(x + y)$ es uno de los números z buscados.

5. Demostrar: Si x y y son racionales positivos, existe un entero positivo p tal que $px > y$.

Sean $x \leftrightarrow [s, m]$ y $y \leftrightarrow [t, n]$ donde s, m, t, n son enteros positivos. Ahora bien, $px > y$ si, y solamente si, $psn > mt$. Como $sn \geq 1$ y $2sn > 1$, la desigualdad queda ciertamente satisfecha si tomamos $p = 2mt$.

6. Demostrar: Todo decimal periódico representa un número racional.

Sea el decimal periódico

$$x{,}yz\overline{def}\ldots = x{,}yz + 0{,}00\overline{def} + 0{,}00000\overline{def} + \cdots$$

Como $x{,}yz$ es un decima limitado, que termina, es una fracción racional, en tanto que $0{,}00\overline{def} + 0{,}00000\overline{def} + \cdots$ es una progresión geométrica infinita cuyo primer término es $a = 0{,}00\overline{def}$, de razón $r = 0{,}001$ y cuya suma es

$$S = \frac{a}{1-r} = \frac{0.00\overline{def}}{0{,}999} = \frac{\overline{def}}{99900}, \quad \text{una fracción racional}$$

Así, pues, siendo la suma de dos números racionales, el decimal periódico es un número racional.

7. Expresar (*a*) $\frac{27}{32}$ en base 4, (*b*) $\frac{1}{3}$ en base 5.

(*a*) $27/32 = 3(\frac{1}{4}) + 3/32 = 3(\frac{1}{4}) + 1(\frac{1}{4})^2 + 1/32 = 3(\frac{1}{4}) + 1(\frac{1}{4})^2 + 2(\frac{1}{4})^3$

La representación pedida es 0,312.

(*b*) $1/3 = 1(\frac{1}{5}) + \frac{2}{15} = 1(\frac{1}{5}) + 3(\frac{1}{5})^2 + 1/75$
$= 1(\frac{1}{5}) + 3(\frac{1}{5})^2 + 1(\frac{1}{5})^3 + 2/375$
$= 1(\frac{1}{5}) + 3(\frac{1}{5})^2 + 1(\frac{1}{5})^3 + 3(\frac{1}{5})^4 + 1/1875$

La representación pedida es $0{,}131313\ldots\ldots$

Problemas propuestos

8. Verificar: (*a*) $[s, m] + [0, n] = [s, m]$ (*c*) $[s, m] + [-s, m] = [0, n] = [s, m] + [s, -m]$
(*b*) $[s, m] \cdot [0, n] = [0, n]$ (*d*) $[s, m] \cdot [m, s] = [n, n]$

9. Enunciar las leyes $\mathbf{A}_1$-$\mathbf{A}_6$, $\mathbf{M}_1$-$\mathbf{M}_5$, $\mathbf{D}_1$-$\mathbf{D}_2$ del Capitulo 4 para números racionales y demostrarlas.

10. Demostrar: (*a*) $\mathscr{F}^+$ es cerrado con respecto a la adición y la multiplicación.
(*b*) Si $[s, m] \in \mathscr{F}^+$, también lo es $[s, m]^{-1}$.

11. Demostrar: (*a*) $\mathscr{F}^-$ es cerrado con respecto a la adición, pero no con respecto a la multiplicación.
(*b*) Si $[s, m] \in \mathscr{F}^-$ también lo es $[s, m]^{-1}$.

12. Demostrar: Si $x, y \in Q$ y $x \cdot y = 0$, es $x = 0$ o $y = 0$.

13. Demostrar: Si $x, y \in Q$, entonces (*a*) $-(x + y) = -x - y$ y (*b*) $-(-x) = x$.

14. Demostrar la ley de tricotomía.

15. Si $x, y, z \in Q$, demostrar:
(*a*) $x + z < y + z$ si, y solo si, $x < y$;
(*b*) si $z > 0$, $xz < yz$ si, y solo si, $x < y$;
(*c*) si $z < 0$, $xz < yz$ si, y solo si, $x > y$.

16. Si $w, x, y, z \in Q$ con $xz \neq 0$ en (*a*) y (*b*), y $xyz \neq 0$ en (*c*), demostrar:
(*a*) $(w : x) \pm (y : z) = (wz \pm xy) : xz$
(*b*) $(w : x) \cdot (y : z) = wy : xz$
(*c*) $(w : x) : (y : z) = wz : xy$

17. Demostrar: Si $a, b \in Q^+$ y $a < b$, es $a^2 < ab < b^2$. ¿Cuál es la desigualdad correspondiente si $a, b \in Q^-$?

Capítulo 7

Los números reales

INTRODUCCION

Los Capítulos 4 y 6 comenzaban con la observación de que el sistema X de números estudiados hasta entonces tenía un defecto manifiesto, defecto que se remediaba ampliando el sistema X. Para lo cual se definía en el conjunto de pares ordenados de elementos de X una relación de equivalencia, etcétera. De ese modo se formaron a partir de N sistemas Z y Q que cumplen $N \subset Z \subset Q$. Para lo que sigue, es de importancia tener presente que cada uno de los nuevos sistemas Z y Q posee una única característica simple, a saber:

Z es el menor conjunto en el cual, para elementos arbitrarios $m, s \in N$, la ecuación $m + x = s$ tiene siempre una solución.

Q es el menor conjunto en el cual, para enteros cualesquiera $m \neq 0$ y s, la ecuación $mx = s$ tiene siempre una solución.

La situación que se presenta ahora no es que Q tenga un defecto solo, pues más bien tiene muchos y tan diversos que el procedimiento de los capítulos anteriores no los remedia todos. Mencionamos dos solamente:

(1) La ecuación $x^3 = 3$ no tiene solución en Q. Porque supóngase lo contrario y que el racional a/b, ya reducido, sea tal que $(a/b)^2 = 3$. Como $a^2 = 3b^2$, se sigue que $3 \mid a^2$ y, por el Teorema V, Capítulo 5, que $3 \mid a$. Escríbase $a = 3a_1$; entonces $3a_1^2 = b^2$ con lo que $3 \mid b^2$ y, por tanto, $3 \mid b$. Pero esto contradice la hipótesis de que a/b era irreducible.

(2) La circunferencia c de un círculo de diámetro $d \in Q$ no es un elemento de Q, esto es, en $c = \pi d$, $\pi \notin Q$. Más aún, $\pi^2 \notin Q$ de modo que π no es solución de $x^2 = q$ para ningún $q \in Q$. (En efecto, π *no* es raíz de ninguna ecuación de la forma $ax^n + bx^{n-1} + \cdots + sx + t = 0$ con $a, b, \ldots, s, t \in Q$.)

El método que se introduce en la sección siguiente para ampliar los números de racionales a reales se debe al matemático alemán R. Dedekind. Con el fin de motivar la definición del concepto fundamental de *cortadura de Dedekind*, o de *cortadura* simplemente en los números racionales, vamos a discutirlo primero en términos no algebraicos.

Considérese el eje racional de la Fig. 7-1, es decir, una recta L en la que los elementos no nulos de Q se asignan a puntos situados a distancias apropiadas (en escala) del origen, que se designa con el 0. Por comodidad, llámese punto racional todo punto de L al que se haya asignado un número racional. (No todo punto de L es punto racional, pues si P es una de las intersecciones del círculo de centro en 0 y radio 2 unidades, con la paralela a L a 1 unidad por encima de ésta y se traza por P la perpendicular a L que la corta en T, entonces, por lo dicho en (1) antes, T no es un punto racional.) Supóngase la recta L dividida en dos partes en alguno de sus puntos. Se presentan dos posibilidades:

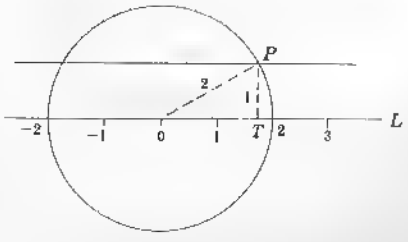


Fig. 7-1

(*a*) El punto en que se divide L no es un punto racional. Entonces, todo punto racional de L está en una de las dos partes, pero no en ambas.

(*b*) El punto en que se divide L es un punto racional. Entonces, con excepción de este punto, cualquier otro punto racional está en una de las partes, pero no en ambas. Convengamos en situar el punto excepcional siempre en la porción derecha.

En cualquiera de los dos casos, el efecto de seccionar L en uno de sus puntos es la determinación de dos subconjuntos propios no vacíos de Q. Como estos subconjuntos son disjuntos en tanto que su unión es Q, cada uno define al otro, y así podemos limitar nuestra atención al subconjunto de la izquierda. Vamos a definir este subconjunto de la izquierda algebraicamente, es decir, sin referencia a ninguna recta.

CORTADURAS DE DEDEKIND

Por *cortadura* C en Q se entiende un subconjunto propio no vacío de Q dotado de las propiedades siguientes:

(i) si $c \in C$ y $a \in Q$ con $a < c$, entonces $a \in C$;
(ii) para todo $c \in C$ existe $b \in C$ tal que $b > c$.

Lo esencial de estas propiedades es que una cortadura no tiene ni elemento mínimo (primero) ni elemento máximo (último). Pero las razones para esto difieren bien claramente: una cortadura C no tiene elemento mínimo porque si $c \in C$, todo número racional $a < c$ es elemento de C. Por otra parte, si bien hay elementos de C mayores que cualquier elemento dado $c \in C$, existen también números racionales mayores que c que *no* pertenecen a C, es decir, que son mayores que todo elemento de C.

Ejemplo 1: Sea r un número racional arbitrario. Demostrar que $C(r) = \{a: a \in Q, a < r\}$ es una cortadura.
Como Q no tiene ni primero ni último elemento, se sigue que existen un $r_1 \in Q$ tal que $r_1 < r$ (luego $C(r) \neq \varnothing$) y un $r_2 \in Q$ tal que $r_2 > r$ (luego $C(r) \neq Q$). Por tanto, $C(r)$ es un subconjunto propio no vacío de Q. Sea $c \in C(r)$, esto es, $c < r$. Entonces, para todo $a \in Q$ tal que $a < c$, se tiene $a < c < r$; así, pues, $a \in C(r)$ como lo exige (i). Y siendo Q denso, existe $d \in Q$ tal que $c < d < r$; con lo que $d > c$ y $d \in C(r)$ como lo exige (ii). $C(r)$ es, pues, una cortadura.

La cortadura definida en el Ejemplo 1 se dirá *cortadura racional*, o, con mayor precisión, *cortadura en el número racional* r. Para un ejemplo de cortadura no racional véase el Problema 1.

Cuando C es una cortadura, se denota por C' el complemento de C en Q. Por ejemplo, si $C = C(r)$ del Ejemplo 1, entonces $C' = C'(r) = \{a': a' \in Q, a' \geq r\}$. Así, pues, el complemento de una cortadura racional es un subconjunto propio de Q que tiene elemento mínimo, pero no máximo. El complemento de la cortadura no racional del Problema 1 carece de elemento máximo, evidentemente; en el Problema 2 se demostrará que no tiene elemento mínimo.

En el Problema 3 se demuestra el

Teorema I. Si C es una cortadura y $r \in Q$, entonces
(*a*) $D = \{r + a: a \in C\}$ es una cortadura y (*b*) $D' = \{r + a': a' \in C'\}$

Ahora es fácil demostrar el

Teorema II. Si C es una cortadura y $r \in Q^+$, entonces
(*a*) $E = \{ra: a \in C\}$ es una cortadura y (*b*) $E' = \{ra': a' \in C'\}$

En el Problema 4 se demuestra el

Teorema III. Si C es una cortadura y $r \in Q^+$, hay un $b \in C$ tal que $r + b \in C'$.

CORTADURAS POSITIVAS

Denótese por $\mathscr{K}$ el conjunto de todas las cortaduras de los números racionales y por $\mathscr{K}^+$ el conjunto de todas las cortaduras (llamadas *cortaduras positivas*) que contienen uno o más elementos de Q^+. Repártanse las restantes cortaduras de $\mathscr{K}$ en la cortadura 0, o sea la $0 = C(0) = \{a: a \in Q^-\}$ y el conjunto $\mathscr{K}^-$ de todas las cortaduras que contienen algún elemento de Q^-, pero no todos. Por ejemplo, $C(2) \in \mathscr{K}^+$, mientras que $C(-5) \in \mathscr{K}^-$. Por ahora limitaremos nuestra atención solo a las cortaduras de $\mathscr{K}^+$ para las cuales es fácil demostrar el

Teorema IV. Si $C \in \mathscr{K}^+$ y $r > 1 \in Q^+$, existe un $c \in C$ tal que $rc \in C$.

Cada $C \in \mathscr{K}^+$ consiste en todos los elementos de Q^-, 0 y (véase Problema 5) en una infinidad de elementos de Q^+. Para cada $C \in \mathscr{K}^+$ defínase $\mathcal{C} = \{a: a \in C, a > 0\}$ y denótese el conjunto de todos los $\mathcal{C}$ por $\mathscr{H}$. Por ejemplo, si $C = C(3)$ entonces $\mathcal{C}(3) = \{a: a \in Q, 0 < a < 3\}$ y C se puede escribir como $C = C(3) = Q^- \cup \{0\} \cup \mathcal{C}(3)$. Nótese que cada $C \in \mathscr{K}^+$ define un único $\mathcal{C} \in \mathscr{H}$ y que, recíprocamente, cada $\mathcal{C} \in \mathscr{H}$ define una única $C \in \mathscr{K}^+$. Acordemos la convención de que si $C_1 \in \mathscr{K}^+$, entonces $C_1 = Q^- \cup \{0\} \cup \mathcal{C}_1$.

Se definen la adición $(+)$ y la multiplicación $(\cdot)$ sobre $\mathscr{K}^+$ como sigue:

$$\begin{aligned} C_1 + C_2 &= Q^- \cup \{0\} \cup (\mathcal{C}_1 + \mathcal{C}_2) \\ C_1 \cdot C_2 &= Q^- \cup \{0\} \cup (\mathcal{C}_1 \cdot \mathcal{C}_2) \end{aligned} \qquad \text{para cualesquiera } C_1, C_2 \in \mathscr{K}^+$$

con

$$\text{(i)} \quad \begin{cases} \mathcal{C}_1 + \mathcal{C}_2 = \{c_1 + c_2 : c_1 \in \mathcal{C}_1,\ c_2 \in \mathcal{C}_2\} \\ \mathcal{C}_1 \cdot \mathcal{C}_2 = \{c_1 \cdot c_2 : c_1 \in \mathcal{C}_1,\ c_2 \in \mathcal{C}_2\} \end{cases}$$

Es fácil ver que tanto $C_1 + C_2$ como $C_1 \cdot C_2$ son elementos de $\mathscr{K}^+$. Además, como

$$C_1 + C_2 = \{a: a \in C_1 + C_2,\ a > 0\}$$

y

$$C_1 \cdot C_2 = \{a: a \in C_1 \cdot C_2,\ a > 0\}$$

se sigue que $\mathscr{K}^+$ es cerrado con respecto a la adición y la multiplicación según se definen en (i).

Ejemplo 2: Comprobar: (*a*) $C(3) + C(7) = C(10)$, (*b*) $C(3)\,C(7) = C(21)$.

Denótese con $\mathcal{C}(3)$ y $\mathcal{C}(7)$, respectivamente los subconjuntos de todos los racionales positivos de $C(3)$ y $C(7)$. Solo hay que verificar entonces que

$$\mathcal{C}(3) + \mathcal{C}(7) = \mathcal{C}(10) \quad \text{y} \quad \mathcal{C}(3) \cdot \mathcal{C}(7) = \mathcal{C}(21)$$

(*a*) Sean $c_1 \in \mathcal{C}(3)$ y $c_2 \in \mathcal{C}(7)$. Como $0 < c_1 < 3$ y $0 < c_2 < 7$, tenemos $0 < c_1 + c_2 < 10$. Con lo que $c_1 + c_2 \in \mathcal{C}(10)$ y $\mathcal{C}(3) + \mathcal{C}(7) \subseteq \mathcal{C}(10)$. Supóngase ahora que $c_3 \in \mathcal{C}(10)$. Entonces, como $0 < c_3 < 10$,

$$0 < \frac{3}{10}c_3 < 3 \quad \text{y} \quad 0 < \frac{7}{10}c_3 < 7$$

esto es, $\frac{3}{10}c_3 \in \mathcal{C}(3)$ y $\frac{7}{10}c_3 \in \mathcal{C}(7)$. Pero $c_3 = \frac{3}{10}c_3 + \frac{7}{10}c_3$; luego, $\mathcal{C}(10) \subseteq \mathcal{C}(3) + \mathcal{C}(7)$. Así, pues, $\mathcal{C}(3) + \mathcal{C}(7) = \mathcal{C}(10)$ según se afirmaba.

(*b*) Para c_1 y c_2 como en (*a*), tenemos $0 < c_1 \cdot c_2 < 21$. Entonces, $c_1 \cdot c_2 \in \mathcal{C}(21$ y $\mathcal{C}(3) \cdot \mathcal{C}(7) \subseteq \mathcal{C}(21)$. Ahora supóngase $c_3 \in \mathcal{C}(21)$ de modo que $0 < c_3 < 21$ y $0 < \frac{c_3}{21} = q < 1$. Escríbase $q = q_1 \cdot q_2$ con $0 < q_1 < 1$ y $0 < q_2 < 1$. Entonces $c_3 = 21q = (3q_1)(7q_2)$ con $0 < 3q_1 < 3$ y $0 < 7q_2 < 7$, esto es, $3q_1 \in \mathcal{C}(3)$ y $7q_2 \in \mathcal{C}(7)$. Entonces, $\mathcal{C}(21) \subseteq \mathcal{C}(3) \cdot \mathcal{C}(7)$ y $\mathcal{C}(3) \cdot \mathcal{C}(7) = \mathcal{C}(21)$ como se afirmaba.

Las leyes $\mathbf{A}_1$-$\mathbf{A}_4$, $\mathbf{M}_1$-$\mathbf{M}_4$, $\mathbf{D}_1$-$\mathbf{D}_2$ sobre $\mathscr{K}^+$ se siguen inmediatamente de las definiciones de la adición y la multiplicación sobre $\mathscr{K}^+$ y del hecho de que estas leyes rigen en Q^+ y, por tanto, en $\mathscr{H}$. Por otra parte, se demuestra fácilmente que $C(1)$ es el neutro multiplicativo, de modo que $\mathbf{M}_5$ también es válida.

SIMETRICOS MULTIPLICATIVOS

Sea ahora una cortadura cualquiera $C = Q^- \cup \{0\} \cup C \in \mathscr{K}^+$ y defínase

$$C^{-1} = \{b: b \in Q^+, b < a^{-1} \text{ para algún } a \in C'\}$$

En el Problema 6 se demuestra:

Si $C = Q^- \cup \{0\} \cup C$ entonces $C^{-1} = Q^- \cup \{0\} \cup C^{-1}$ es una cortadura positiva.

En el Problema 7 se demuestra:

Para toda $C \in \mathscr{K}^+$, su simétrica multiplicativa es $C^{-1} \in \mathscr{K}^+$.

Ahora se puede elegir entre dos vías para sumergir $\mathscr{K}^+$ en un sistema en que cada elemento tenga un simétrico aditivo:

(1) Repetir lo del Capítulo 4 poniendo $\mathscr{K}^+$ en lugar de N.
(2) O bien identificar cada elemento de $\mathscr{K}^-$ como el simétrico aditivo de un elemento único de $\mathscr{K}^+$. Procederemos de esta manera.

SIMETRICOS ADITIVOS

La definición de la suma de dos cortaduras positivas es equivalente a

$$C_1 + C_2 = \{c_1 + c_2: c_1 \in C_1, c_2 \in C_2\}, \qquad C_1, C_2 \in \mathscr{K}^+$$

Se generaliza la definición para abarcar todas las cortaduras así:

$$C_1 + C_2 = \{c_1 + c_2: c_1 \in C_1, c_2 \in C_2\}, \qquad C_1, C_2 \in \mathscr{K} \tag{1}$$

Ejemplo 3: Comprobar que $C(3) + C(-7) = C(-4)$.

Sea $c_1 + c_2 \in C(3) + C(-7)$, donde $c_1 \in C(3)$ y $c_2 \in C(-7)$. Como $c_1 < 3$ y $c_2 < -7$, se sigue que $c_1 + c_2 < -4$ de modo que $c_1 + c_2 \in C(-4)$. Así, pues, $C(3) + C(-7) \subseteq C(-4)$.

Recíprocamente, sea $c_3 \in C(-4)$. Entonces, $c_3 < -4$ y $-4 - c_3 = d \in Q^+$. Ahora bien, $c_3 = -4 - d = (3 - \frac{1}{2}d) + (-7 - \frac{1}{2}d)$; entonces, como $3 - \frac{1}{2}d \in C(3)$ y $-7 - \frac{1}{2}d \in C(-7)$, se sigue que $c_3 \in C(3) + C(-7)$ y es $C(-4) \subseteq C(3) + C(-7)$. Así que $C(3) + C(-7) = C(-4)$ como se quería.

Ahora, para cada $C \in \mathscr{K}$, defínase

$$-C = \{x: x \in Q, x < -a \text{ para algún } a \in C'\}$$

Para $C = C(-3)$, se tiene $-C = \{x: x \in Q, x < 3\}$ porque -3 es el elemento mínimo de C'. Pero ésta es precisamente $C(3)$; luego, en general,

$$-C(r) = C(-r) \qquad \text{si } r \in Q$$

En el Problema 8 se demuestra que $-C$ es ciertamente una cortadura, y en el Problema 9, que $-C$ es la simétrica aditiva de C. Entonces, las leyes $\mathbf{A}_1$-$\mathbf{A}_4$ se cumplen en $\mathscr{K}$.

En el Problema 10 se demuestra la

Ley de tricotomía. Para toda $C \in \mathscr{K}$, se verifica una, y solamente una, de las relaciones

$$C = C(0) \qquad C \in \mathscr{K}^+ \qquad -C \in \mathscr{K}^+$$

MULTIPLICACION SOBRE $\mathscr{K}$

Para toda $C \in \mathscr{K}$, se define

$$C > C(0) \quad \text{si, y solo si,} \quad C \in \mathscr{K}^+$$
$$C < C(0) \quad \text{si, y solo si,} \quad -C \in \mathscr{K}^+$$

y
$$|C| = C \quad \text{si} \quad C \geq C(0)$$
$$|C| = -C \quad \text{si} \quad C < C(0)$$

Así, $|C| \geq C(0)$, es decir, $|C| = C(0)$ o $|C| \in \mathcal{K}^+$.

Para todo $C_1, C_2 \in \mathcal{K}$, se defina

$$\begin{cases} C_1 \cdot C_2 = C(0) & \text{si} \quad C_1 = C(0) \text{ o bien } C_2 = C(0) \\ C_1 \cdot C_2 = |C_1| \cdot |C_2| & \text{si} \quad C_1 > C(0) \text{ y } C_2 > C(0) \text{ o si } C_1 < C(0) \text{ y } C_2 < C(0) \\ C_1 \cdot C_2 = -(|C_1| \cdot |C_2|) & \text{si} \quad C_1 > C(0) \text{ y } C_2 < C(0) \text{ o si } C_1 < C(0) \text{ y } C_2 > C(0) \end{cases} \tag{2}$$

Finalmente, para $C \neq C(0)$, definimos

$$C^{-1} = |C|^{-1} \quad \text{si} \quad C > C(0) \qquad \text{y} \qquad C^{-1} = -(|C|^{-1}) \quad \text{si} \quad C < C(0)$$

Ahora resulta fácilmente que las leyes $\mathbf{A}_1$-$\mathbf{A}_6$, $\mathbf{M}_1$-$\mathbf{M}_6$, $\mathbf{D}_1$-$\mathbf{D}_2$ (véase página 71) rigen en $\mathcal{K}$.

SUSTRACCION Y DIVISION

En forma análoga a la de la sección correspondiente del Capítulo 6, se define para cualesquiera $C_1, C_2 \in \mathcal{K}$

$$C_1 - C_2 = C_1 + (-C_2) \tag{3}$$

y, si $C_2 \neq C(0)$,

$$C_1 : C_2 = C_1 \cdot C_2^{-1} \tag{4}$$

Nota. Nos encontramos a esta altura en la incómoda situación de disponer de dos significados completamente diferentes de $C_1 - C_2$. En todo este capítulo convendremos, pues, en considerar $C_1 - C_2$ y $C_1 \cap C_2'$ como expresiones con significados diferentes.

RELACIONES DE ORDEN

Para cualesquiera dos cortaduras distintas $C_1, C_2 \in \mathcal{K}$ se define

$$C_1 < C_2, \text{ o también } C_2 > C_1, \text{ significa } C_1 - C_2 < C(0)$$

En el Problema 11 se demuestra que

$$C_1 < C_2, \text{ o también } C_2 > C_1, \text{ si, y solo si, } C_1 \subset C_2$$

Se sigue fácilmente la

Ley de tricotomía. Para cualesquiera $C_1, C_2 \in \mathcal{K}$ se verifica una, y solo una, de las siguientes relaciones:

$$(a)\ C_1 = C_2 \qquad (b)\ C_1 < C_2 \qquad (c)\ C_1 > C_2$$

PROPIEDADES DE LOS NUMEROS REALES

Defínase $\mathcal{K}^* = \{C(r): C(r) \in \mathcal{K}, r \in Q\}$. Se deja al lector la demostración del

Teorema V. La aplicación $C(r) \in \mathcal{K}^* \to r \in Q$ es un isomorfismo de $\mathcal{K}^*$ sobre Q.

Los elementos de $\mathcal{K}$ se llaman *números reales*, y cuando quiera que sea más cómodo, $\mathcal{K}$ se remplazará por el familiar R, mientras que $A, B, \ldots$, denotarán elementos arbitrarios de R. Ahora bien, $Q \subset R$; los elementos del complemento de Q en R se llaman *números irracionales*.

En los Problemas 12 y 13 se demuestran la

Propiedad de densidad. Si $A, B \in R$ con $A < B$, existe un número racional $C(r)$ tal que $A < C(r) < B$.

y la

Propiedad arquimediana. Si $A, B \in R^+$ existe un entero positivo $C(n)$ tal que $C(n) \cdot A > B$.

A fin de establecer en lo que sigue una importante propiedad de los números reales que no existe para los números racionales, se hace la definición:

Sea $S \neq \varnothing$ un conjunto en el cual está bien definida la relación de orden $<$, y sea T cualquier subconjunto propio de S. Un elemento $s \in S$, si existe, tal que $s \geq t$ para todo $t \in T$ ($s \leq t$ para todo $t \in T$) se llama *mayorante* (*minorante*) de T.

Ejemplo 4: (*a*) Si $S = Q$ y $T = \{-5, -1, 0, 1, 3/2\}$, entonces $3/2$, 2, $\sqrt{2}, \ldots$ son mayorantes de T, en tanto que -5, $-17/3$, $-100, \ldots$, son minorantes de T.

(*b*) Si $S = Q$ y $T = C \in \mathscr{K}$ entonces T no tiene minorante en tanto que cualquier $t' \in T' = C'$ es un mayorante. Por otra parte, T' carece de mayorante, mientras que cualquier $t \in T$ es un minorante.

Si el conjunto de todos los mayorantes (minorantes) de un subconjunto T de un conjunto S contiene un elemento mínimo (un elemento máximo) e, se dice que e es el *extremo superior* (*extremo inferior*) de T.

Sea Q el conjunto universal y considérese la cortadura racional $C(r) \in \mathscr{K}$. Como r es el elemento mínimo de $C'(r)$, todo $s \geq r$ en Q es un mayorante de $C(r)$ y todo $t \leq r$ en Q es un minorante de $C'(r)$. Así, pues, r es el extremo superior de $C(r)$ y el extremo inferior de $C'(r)$.

Ejemplo 5: (*a*) El conjunto T del Ejemplo 4(*a*) tiene el $3/2$ como extremo superior y el -5 como extremo inferior.

(*b*) Sea Q el conjunto universal. La cortadura C del Problema 1 carece de minorantes y, por tanto, de extremo inferior. Si bien tiene mayorantes, no tiene extremo superior porque C no tiene elemento máximo y C' no tiene elemento mínimo.

(*c*) Sea R el conjunto universal. Siendo cualquier cortadura $C \in \mathscr{K}$ un subconjunto de Q, es un subconjunto de R. La cortadura $C(r)$ tiene entonces mayorantes en R y $r \in R$ como extremo superior. Asimismo, la cortadura C del Problema 1 tiene mayorantes en R y $\sqrt{3} \in R$ como extremo superior.

El Ejemplo 5(*c*) ilustra el

Teorema VI. Si $\mathbb{S}$ es un subconjunto no vacío de $\mathscr{K}$ y si $\mathbb{S}$ tiene un mayorante en $\mathscr{K}$, tiene un extremo superior en $\mathscr{K}$.

Para una demostración, véase Problema 14.

Análogamente, se tiene el

Teorema VI'. Si $\mathbb{S}$ es un subconjunto no vacío de $\mathscr{K}$ y $\mathbb{S}$ tiene un minorante en $\mathscr{K}$, tiene un extremo inferior en $\mathscr{K}$.

Así, pues, el conjunto R de los números reales tiene la

Propiedad de plenitud. Todo subconjunto no vacío de R que tenga un minorante (mayorante) tiene un extremo inferior (superior).

Supóngase $\theta^n = \alpha$ donde $\alpha, \theta \in R^+$ y $n \in Z^+$. Se dice que θ es la raíz *enésima* principal de α y se escribe $\theta = \alpha^{1/n}$. Entonces, para $r = m/n \in Q$ se sigue que $\alpha^r = \theta^m$.

Otras propiedades de R son:

(1) Para todo $\alpha \in R^+$ y todo $n \in Z^+$ existe un único $\theta \in R^+$ tal que $\theta^n = \alpha$.

(2) Para números reales $\alpha > 1$ y β, defínase α^β como el extremo superior de $\{\alpha^r : r \in Q, r < \beta\}$. Entonces, α^β está definida para todo $\alpha > 0$, $\beta \in R$ haciendo $\alpha^\beta = (1/\alpha)^{-\beta}$ si $0 < \alpha < 1$.

RESUMEN

Como resumen parcial hasta el momento, he aquí una lista de las propiedades fundamentales del sistema R de los números reales. A la derecha, entre paréntesis, se indican otros sistemas, N, Z, Q, en los que rige cada propiedad dada.

Adición

A_1.	Ley de clausura	$r + s \in R$, para cualesquiera $r, s \in R$.	(N, Z, Q)
A_2.	Ley conmutativa	$r + s = s + r$, para cualesquiera $r, s \in R$.	(N, Z, Q)
A_3.	Ley asociativa	$r + (s + t) = (r + s) + t$, para cualesquiera $r, s, t \in R$.	(N, Z, Q)
A_4.	Ley de cancelación	Si $r + t = s + t$, es $r = s$ para cualesquiera $r, s, t \in R$	(N, Z, Q)
A_5.	Neutro aditivo	Existe un elemento neutro aditivo único $0 \in R$ tal que $r + 0 = 0 + r = r$, para todo $r \in R$.	(Z, Q)
A_6.	Simétrico aditivo	Para cada $r \in R$ existe un único simétrico aditivo, llamado opuesto, $-r \in R$ tal que $r + (-r) = (-r) + r = 0$.	(Z, Q)

Multiplicación

M_1.	Ley de clausura	$r \cdot s \in R$, para cualesquiera $r, s \in R$.	(N, Z, Q)
M_2.	Ley conmutativa.	$r \cdot s = s \cdot r$, para cualesquiera $r, s \in R$	(N, Z, Q)
M_3.	Ley asociativa	$r \cdot (s \cdot t) = (r \cdot s) \cdot t$, para cualesquiera $r, s, t \in R$.	(N, Z, Q)
M_4.	Ley de cancelación	Si $m \cdot p = n \cdot p$, entonces $m = n$ para cualesquiera $m, n \in R$ y $p \neq 0 \in R$.	(N, Z, Q)
M_5.	Neutro multiplicativo	Existe un elemento neutro multiplicativo único $1 \in R$ tal que $1 \cdot r = r \cdot 1 = r$ para todo $r \in R$.	(N, Z, Q)
M_6.	Simétrico multiplicativo.	Para cada $r \neq 0 \in R$ existe un único simétrico multiplicativo $r^{-1} \in R$ tal que $r \cdot r^{-1} = r^{-1} \cdot r = 1$.	(Q)

Leyes distributivas		Para cualesquiera $r, s, t \in R$,	
D_1.		$r \cdot (s + t) = r \cdot s + r \cdot t$	
D_2.		$(s + t) \cdot r = s \cdot r + t \cdot r$	(N, Z, Q)
Propiedad de densidad		Para todo $r, s \in R$, con $r < s$, existe $t \in Q$ tal que $r < t < s$.	(Q)
Propiedad arquimediana		Para todo $r, s \in R^+$, con $r < s$, existe $n \in Z^+$ tal que $n \cdot r > s$.	(Q)
Propiedad de plenitud		Todo subconjunto no vacío de R que tenga un minorante (mayorante) tiene un extremo inferior (extremo superior).	(N, Z)

Problemas resueltos

1. Demostrar que el conjunto S formado por Q^-, cero y todos los $s \in Q^+$ tales que $s^2 < 3$, es una cortadura.

Primero que todo, S es un subconjunto propio de Q, pues $1 \in S$ y $2 \notin S$. En segundo lugar, sean $c \in S$ y $a \in Q$ con $a < c$. Evidentemente, $a \in S$ si $a \leq 0$ y también si $c \leq 0$.

Para el caso restante ($0 < a < c$), $a^2 < ac < c^2 < 3$; luego $a^2 < 3$ y $a \in S$ como se requiere en (i), página 66. La propiedad (ii), página 66, queda cumplida por $b = 1$ si $c \leq 0$; entonces S será una cortadura siempre que para cada $c > 0$, con $c^2 < 3$ pueda hallarse siempre un $m \in Q^+$ tal que $(c + m)^2 < 3$. Se pueden simplificar un tanto las cosas notando que si p/q, donde $p, q \in Z^+$ ha de ser un m semejante, también lo es $1/q$. Pero $q \geq 1$; luego $\left(c + \frac{1}{q}\right)^2 = c^2 + \frac{2c}{q} + \frac{1}{q^2} \leq c^2 + \frac{2c+1}{q}$; así, pues, $\left(c + \frac{1}{q}\right)^2 < 3$ siempre que $\frac{2c+1}{q} < 3 - c^2$, esto es, siempre que $(3 - c^2)q > 2c + 1$. Como $(3 - c^2) \in Q^+$ y $(2c + 1) \in Q^+$, la existencia de $q \in Z^+$ que cumpla la última desigualdad viene asegurada por la propiedad arquimediana de Q^+. Así, pues, S es una cortadura.

2. Demuéstrese que el complemento S' del conjunto S del Problema 1 carece de elemento mínimo.

Para todo $r \in S' = \{a: a \in Q^+, a^2 \geq 3\}$, vamos a demostrar que se puede hallar siempre un número racional positivo m tal que $(r - m)^2 > 3$, esto es, que el r que se elija nunca podrá ser elemento mínimo de S'. Como en el Problema 1, por simplificar, se busca un m de la forma $1/q$ con $q \in Z^+$. Así se tiene $\left(r - \frac{1}{q}\right)^2 = r^2 - \frac{2r}{q} + \frac{1}{q^2} > r^2 - \frac{2r}{q}$; luego $\left(r - \frac{1}{q}\right)^2 > 3$ siempre que $\frac{2r}{q} < r^2 - 3$, esto es, siempre que $(r^2 - 3)q > 2r$. Como en el Problema 1, la propiedad arquimediana de Q^+ asegura la existencia de $q \in Z^+$ que satisfaga la última desigualdad. Así que S' carece de elemento mínimo.

3. Demostrar: Si C es una cortadura y $r \in Q$, entonces (a) $D = \{r + a: a \in C\}$ es una cortadura y (b) $D' = \{r + a': a' \in C'\}$.

(a) $D \neq \emptyset$ porque $C \neq \emptyset$; además, para todo $c' \in C'$, $r + c' \notin D$ y $D \neq Q$. Luego D es un subconjunto propio de Q.

Sea $b \in C$. Para cualquier $s \in Q$ tal que $s < r + b$, se tiene $s - r < b$ de modo que $s - r \in C$ y entonces $s = r + (s - r) \in D$ según la condición de (i), página 66. Así que para $b \in C$ existe un elemento $c \in C$ tal que $c > b$; luego $r + b$, $r + c \in D$ y $r + c > r + b$ como se pide en (ii), página 66. De modo que D es una cortadura.

(b) Sea $b' \in C'$. Entonces $r + b' \notin D$ porque $b' \notin C$; luego $r + b' \in D'$. Por otra parte, si $q' = r + p' \in D'$ entonces $p' \notin C$, pues si perteneciera tendríamos $D \cap D' \neq \emptyset$. Así que D' es lo definido.

4. Demostrar: Si C es una cortadura y $r \in Q^+$, existe un $b \in C$ tal que $r + b \in C'$.

Según el Problema 3, $D = \{r + a: a \in C\}$ es una cortadura. Como $r > 0$, se sigue que $C \subset D$. Sea $q \in Q$ tal que $p = r + q \in D$ pero no de C. Entonces $q \in C$ pero $r + q \in C'$. Así, pues, q satisface los requisitos de b en el teorema.

5. Demostrar: Si $C \in \mathscr{K}^+$, C contiene infinitos elementos de Q^+.

Como $C \in \mathscr{K}^+$ existe al menos un $r \in Q^+$ tal que $r \in C$. Entonces para todo $q \in N$ se tiene $r/q \in C$. Así, pues, ningún $C \in \mathscr{K}^+$ contiene solamente un número finito de racionales positivos.

6. Demostrar: Si $C = Q^- \cup \{0\} \cup \mathcal{C} \in \mathscr{K}^+$, entonces $C^{-1} = Q^- \cup \{0\} \cup \mathcal{C}^{-1}$ es una cortadura positiva.

Como $\mathcal{C} \neq Q^+$ se sigue que $C' \neq \emptyset$ y como $\mathcal{C} \neq \emptyset$, resulta que $C' \neq Q^+$. Sea $d \in C'$. Entonces $(d + 1)^{-1} \in Q^+$ y $(d + 1)^{-1} < d^{-1}$ de modo que $(d + 1)^{-1} \in \mathcal{C}^{-1}$ y $\mathcal{C}^{-1} \neq \emptyset$. Así, si $c \in C$, entonces para todo $a \in C'$ se tiene $c < a$ y $c^{-1} > a^{-1}$; luego $c^{-1} \notin \mathcal{C}^{-1}$ y $\mathcal{C}^{-1} \neq Q^+$. Así que C^{-1} es un subconjunto propio de Q.

Sean $c \in \mathcal{C}^{-1}$ y $r \in Q^+$ tales que $r < c$. Entonces $r < c < d^{-1}$ para algún $d \in C'$ y $r \in \mathcal{C}^{-1}$ como se requiere en (i), página 66. Asimismo, como $c \neq d^{-1}$ existe $s \in Q^+$ tal que $c < s < d^{-1}$ y $s \in \mathcal{C}^{-1}$ como se requiere en (ii). De modo que C^{-1} es una cortadura positiva.

7. Demostrar: Para cada $C \in \mathscr{K}^+$, su simétrica multiplicativa es $C^{-1} \in \mathscr{K}^+$.

Sea $C = Q^- \cup \{0\} \cup \mathcal{C}$ de modo que $C^{-1} = Q^- \cup \{0\} \cup \mathcal{C}^{-1}$. Entonces $\mathcal{C} \cdot \mathcal{C}^{-1} = \{c \cdot b: c \in \mathcal{C}, b \in \mathcal{C}^{-1}\}$. Pero $b < d^{-1}$ para algún $d \in C'$ y entonces $bd < 1$; asimismo, $c < d$ de modo que $bc < 1$. Por tanto, $\mathcal{C} \cdot \mathcal{C}^{-1} \subseteq \mathcal{C}(1)$.

Sea $n \in \mathcal{C}(1)$ tal que $n^{-1} > 1$. Por el Teorema IV, existe $c \in C$ tal que $c \cdot n^{-1} \in C'$. Para cada $a \in C$ tal que $a > c$, se tiene $n \cdot a^{-1} < n \cdot c^{-1} = (c \cdot n^{-1})^{-1}$; así que $n \cdot a^{-1} = e \in \mathcal{C}^{-1}$. Luego $n = ae \in C \cdot \mathcal{C}^{-1}$ y $\mathcal{C}(1) \subseteq \mathcal{C} \cdot \mathcal{C}^{-1}$. Por consiguiente, $\mathcal{C} \cdot \mathcal{C}^{-1} = \mathcal{C}(1)$ y $C \cdot \mathcal{C}^{-1} = C(1)$. Por el Problema 6, es $C^{-1} \in \mathscr{K}^+$.

8. Si $C \in \mathscr{K}$, demostrar que $-C$ es una cortadura.

Nótese primero que $-C \neq \emptyset$ puesto que $C' \neq \emptyset$. Sea ahora $c \in C$; entonces $-c \notin -C$ pues si lo fuera se tendría $-c < -c'$ (para algún $c' \in C'$) de modo que $c' < c$, una contradicción. Así que $-C$ es un subconjunto propio de Q. La propiedad (i), página 66, es inmediata. Para demostrar la propiedad (ii), sea $x \in -C$, esto es $x < -c'$ para algún $c' \in C'$. Pero $x < \frac{1}{2}(x - c') < -c'$. Así, pues, $\frac{1}{2}(x - c') > x$ y $\frac{1}{2}(x - c') \in -C$.

9. Demostrar que $-C$ del Problema 8 es la simétrica aditiva de C, esto es, que $C + (-C) = -C + C = C(0)$.

Sea $c + x \in C + (-C)$, con $c \in C$ y $x \in -C$. Ahora bien, si $x < -c'$ para $c' \in C'$, se tiene $c + x < c - c' < 0$ puesto que $c < c'$. Entonces, $C + (-C) \subseteq C(0)$. Recíprocamente, sean y, $z \in C(0)$ con $z > y$. Entonces, por el Teorema III, existen $c \in C$ y $c' \in C'$ tales que $c + (z - y) = c'$. Como $z - c' < -c'$, se sigue que $z - c' \in -C$. Así que $y = c + (z - c') \in C + (-C)$ y $C(0) \subseteq C + (-C)$. Luego $C + (-C) = -C + C = C(0)$.

10. Demostrar la ley de tricotomía: Para $C \in \mathscr{K}$ se verifica una, y solo una, de las relaciones

$$C = C(0) \qquad C \in \mathscr{K}^+ \qquad -C \in \mathscr{K}^+$$

Es claro que ni $C(0)$ ni $-C(0) \in \mathscr{K}^+$. Supóngase ahora que $C \neq C(0)$ y $C \notin \mathscr{K}^+$. Como todo $c \in C$ es un número racional negativo pero $C \neq Q^-$, existe $c' \in Q^-$ tal que $c' \in C'$. Como $c' < \frac{1}{2}c' < 0$, se sigue que $0 < -\frac{1}{2}c' < -c'$. Entonces, $-\frac{1}{2}c' \in -C$ y así $C \in \mathscr{K}^+$. Por el contrario, si $C \in \mathscr{K}^+$, todo $c' \in C'$ es también $\in Q^+$. Luego todo elemento de $-C$ es negativo y $-C \notin \mathscr{K}^+$.

11. Demostrar: Para dos cortaduras cualesquiera C_1, $C_2 \in \mathscr{K}$ se tiene $C_1 < C_2$ si, y solo si, $C_1 \subset C_2$.

Supóngase $C_1 \subset C_2$. Elíjase $a' \in C_2 \cap C_1'$ y luego $b \in C_2$ tal que $b > a'$. Como $-b < -a'$, se sigue que $-b \in -C_1$. Pero $-C_1$ es una cortadura; luego existe un elemento $c \in -C_1$ tal que $c > -b$. Entonces $b + c > 0$ y $b + c \in C_2 + (-C_1) = C_2 - C_1$ de modo que $C_2 - C_1 \in \mathscr{K}^+$. Así, pues, $C_2 - C_1 > C(0)$ y $C_1 < C_2$.

Para la recíproca, supóngase $C_1 < C_2$. Entonces, $C_2 - C_1 > C(0)$ y $C_2 - C_1 \in \mathscr{K}^+$. Elíjase $d \in Q^+$ tal que $d \in C_2 - C_1$ y escríbase $d = b + a$ con $b \in C_2$ y $a \in -C_1$. Entonces, $-b < -a'$ porque $d > 0$ y como $a \in -C_1$ podemos elegir un $a' \in C_1'$ tal que $a < -a'$. Pero $-b < -a'$; entonces, $a' < b$, de modo que $b \notin C_1$, y así, pues, $C_2 \not\subseteq C_1$. Ahora considérese cualquier $x \in C_1$. Entonces, $x < b$ de modo que $x \in C_2$ y, por tanto, $C_1 \subset C_2$.

12. Demostrar: Si A, $B \in R$ con $A < B$ existe un número racional $C(r)$ tal que $A < C(r) < B$.

Como $A < B$, existen números racionales r y s con $r < s$ tales que $r, s \in B$, pero de A. Entonces, $A < C(s) < C(r) < B$, como se pedía.

13. Demostrar: Si A, $B \in R^+$ existe un entero positivo $C(n)$ tal que $C(n) \cdot A > B$.

Como esto es trivial para $A > B$, supóngase $A < B$. Sean r, s números racionales positivos tales que $r \in A$ y $s \in B'$; entonces $C(r) < A$ y $C(s) > B$. Por la propiedad arquimediana de Q existe un número positivo n tal que $nr > s$, es decir, $C(n) \cdot C(r) > C(s)$. Luego

$$C(n) \cdot A > C(n) \cdot C(r) > C(s) > B$$

como se pedía.

14. Demostrar: Si $\mathbb{S}$ es un subconjunto no vacío de $\mathscr{K}$ y si $\mathbb{S}$ tiene un mayorante (en $\mathscr{K}$), tiene extremo superior en $\mathscr{K}$.

Sea $\mathbb{S} = \{C_1, C_2, C_3, \ldots\}$ el dicho subconjunto y C un mayorante. La unión $U = C_1 \cup C_2 \cup C_3 \cup \ldots$ de las cortaduras de $\mathbb{S}$ es ella misma una cortadura $\in \mathscr{K}$; asimismo, como $C_1 \subseteq U$, $C_2 \subseteq U$, $C_3 \subseteq U$, $\ldots$, U es un mayorante de $\mathbb{S}$. Pero $C_1 \subseteq C$, $C_2 \subseteq C$, $C_3 \subseteq C$, $\ldots$; luego $U \subseteq C$ y U es el extremo superior de $\mathbb{S}$.

Problemas propuestos

15. (*a*) Definir $C(3)$ y $C(-7)$. Demostrar que cada una es una cortadura.
(*b*) Definir $C'(3)$ y $C'(-7)$.
(*c*) Situar -10, -5, 0, 1, 4 como $\in$ o $\notin$ de $C(3)$, $C(-7)$, $C'(3)$, $C'(-7)$.
(*d*) Hallar 5 números racionales de $C(3)$ que no estén en $C(-7)$.

16. Demostrar: $C(r) \subset C(s)$ si, y solamente si, $r < s$.

17. Demostrar: Si A y B son cortaduras, entonces $A \subset B$ implica $A \neq B$.

18. Demostrar el Teorema II de la página 66.

19. Demostrar: Si C es una cortadura y $r \in Q^+$, entonces $C \leq D = \{a + r: a \in C\}$.

20. Demostrar el Teorema IV, página 67.

21. Sea $r \in Q$, pero no de $C \in \mathscr{K}$. Demostrar que $C \leq C(r)$.

22. Demostrar: (*a*) $C(2) + C(5) = C(7)$ (*c*) $C(r) + C(0) = C(r)$
(*b*) $C(2) \cdot C(5) = C(10)$ (*d*) $C(r) \cdot C(1) = C(r)$

23. Demostrar: (*a*) Si $C \in \mathscr{K}^+$, es $-C \in \mathscr{K}^-$.
(*b*) Si $C \in \mathscr{K}^-$, es $-C \in \mathscr{K}^+$.

24. Demostrar: $-(-C) = C$

25. Demostrar: (*a*) Si $C_1, C_2 \in \mathscr{K}$, entonces $C_1 + C_2$ y $|C_1| \cdot |C_2|$ son cortaduras.
(*b*) Si $C_1 \neq C(0)$, entonces $|C_1|^{-1}$ es una cortadura.
(*c*) $(C^{-1})^{-1} = C$ para todo $C \neq C(0)$.

26. Demostrar: (*a*) Si $C \in \mathscr{K}^+$, entonces $C^{-1} \in \mathscr{K}^+$.
(*b*) Si $C \in \mathscr{K}^-$, entonces $C^{-1} \in \mathscr{K}^-$.

27. Demostrar: Si $r, s \in Q$ con $r < s$ existe un número irracional α tal que $r < \alpha < s$.

Sugerencia: Considérese $\alpha = r + \dfrac{s - r}{\sqrt{2}}$.

28. Demostrar: Si A y B son números reales con $A < B$, existe un número irracional α tal que $A < \alpha < B$.

Sugerencia: Utilícese el Problema 12 para demostrar: Si A y B son números reales con $A < B$, existen números racionales t y r tales que $A < C(t) < C(r) < B$.

29. Demostrar el Teorema V, página 69.

Capítulo 8

Los números complejos

EL SISTEMA C DE LOS NUMEROS COMPLEJOS

El sistema C de los números complejos es el sistema de números del álgebra ordinaria. Es el mínimo conjunto en que, por ejemplo, la ecuación $x^2 = a$ se puede resolver cuando a es un elemento cualquiera de R. Para construir este conjunto C, comenzaremos con el conjunto producto $R \times R$. La relación binaria «=» se define así:

$$(a, b) = (c, d) \quad \text{si, y solo si,} \quad a = c \text{ y } b = d$$

Como ahora cada una de las clases de equivalencia resultantes no contiene más que un solo elemento, denotaremos estas clases (a, b) en vez de $[a, b]$ y denotaremos en lo sucesivo $R \times R$ por C.

ADICION Y MULTIPLICACION SOBRE C

La adición y la multiplicación sobre C se definen respectivamente por

$$\text{(i)} \qquad (a, b) + (c, d) = (a + c, b + d)$$

$$\text{(ii)} \qquad (a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

para cualesquiera $(a, b), (c, d) \in C$

Los cálculos necesarios para demostrar que estas operaciones siguen las leyes $\mathbf{A}_1$-$\mathbf{A}_4$, $\mathbf{M}_1$-$\mathbf{M}_4$, $\mathbf{D}_1$-$\mathbf{D}_2$ del Capítulo 7, cuando se las enuncia en términos de C, son de rutina y se dejan al lector. Es fácil verificar que $(0, 0)$ es el elemento neutro para la adición y que $(1, 0)$ es el elemento neutro para la multiplicación; también que el simétrico aditivo de (a, b) es el elemento $-(a, b) = (-a, -b)$ y que el simétrico multiplicativo de $(a, b) \neq (0, 0)$ es el $(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right)$. Así, pues, el conjunto de los números complejos tiene las propiedades $\mathbf{A}_5$-$\mathbf{A}_6$ y $\mathbf{M}_5$-$\mathbf{M}_6$ del Capítulo 7, enunciadas ahora en términos de C.

En la sección siguiente demostraremos que $R \subset C$; y se podría esperar entonces que C tenga todas las propiedades fundamentales de R. Pero esto no es cierto, puesto que no es posible generalizar a C (definir en C) la relación de orden «<» de R para todos los elementos de C.

Véase Problema 1.

PLOPIEDADES DE LOS NUMEROS COMPLEJOS

Los números reales son un subconjunto propio de los números complejos C. Porque si en (i) y (ii) hacemos $b = d = 0$, se ve que las primeras componentes se combinan exactamente como los números reales a y c. Así, pues, la aplicación $a \leftrightarrow (a, 0)$ es un isomorfismo de R sobre un cierto subconjunto $\{(a, b): a \in R, b = 0\}$ de C.

Los elementos $(a, b) \in C$ en los que $b \neq 0$ se dicen *números imaginarios* y si $a = 0$, (a, b) es *un número imaginario puro*.

Para cada número complejo $z = (a, b)$ se define el número complejo $\bar{z} = \overline{(a, b)} = (a, -b)$ que se llama *conjugado* del z. Evidentemente, todo número real es su propio conjugado en tanto que el conjugado de un imaginario puro es su opuesto.

De aquí se sigue fácilmente:

Teorema I. La suma (producto) de dos complejos conjugados es real.

Teorema II. El cuadrado de todo número imaginario puro es un número real negativo.

Véase también Problema 2.

El papel especial del número complejo (1, 0) sugiere investigar el de otro, (0, 1). Se tiene

$$(x, y) \cdot (0, 1) = (-y, x) \quad \text{para todo} \quad (x, y) \in C$$

y, en particular,

$$(y, 0) \cdot (0, 1) = (0, 1) \cdot (y, 0) = (0, y)$$

Además, $(0, 1)^2 = (0, 1) \cdot (0, 1) = (-1, 0) \leftrightarrow -1$ en la anterior aplicación, de modo que (0, 1) es una solución de $z^2 = -1$.

Definiendo (0, 1) como la *unidad imaginaria* y denotándola por i, se tiene

$$i^2 = -1$$

y, para todo $(x, y) \in C$,

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (y, 0) \cdot (0, 1) = x + yi$$

En esta notación más familiar, x se llama *parte real* y y *parte imaginaria* del número complejo. Resumiendo:

el opuesto de $z = x + yi$ es $-z = -(x + yi) = -x - yi$

el conjugado de $z = x + yi$ es $\bar{z} = \overline{x + yi} = x - yi$

para todo $z = x + yi$, $z \cdot \bar{z} = x^2 + y^2 \in R$

para todo $z \neq 0 + 0 \cdot i = 0$, $z^{-1} = \dfrac{1}{z} = \dfrac{\bar{z}}{z \cdot \bar{z}} = \dfrac{x}{x^2 + y^2} - \dfrac{y}{x^2 + y^2} i$.

SUSTRACCION Y DIVISION SOBRE C

La sustracción y la división sobre C se definen por

(iii) $z - w = z + (-w)$ para cualesquiera $z, w \in C$

(iv) $z : w = z \cdot w^{-1}$, para cualesquiera $w \neq 0$, $z \in C$

REPRESENTACION TRIGONOMETRICA

La representación de un número complejo z por (x, y) y por $x + yi$ sugiere la aplicación (isomorfismo)

$$x + yi \leftrightarrow (x, y)$$

del conjunto C de los números complejos sobre los puntos del plano real. Podemos, pues, hablar del punto $P(x, y)$ o $P(x + yi)$ como mejor convenga a nuestro propósito del momento. El empleo de una sola coordenada simplifica, a menudo, muchos cálculos que de otro modo serían tediosos. En seguida se discute un ejemplo de ello y otro se esquematiza brevemente en el Problema 20.

Considérese en la Fig. 8-1 el punto $P(x + yi) \neq 0$ cuya distancia r a O viene dada por $r = \sqrt{x^2 + y^2}$. Si θ es el ángulo positivo que OP hace con el eje positivo de las x, se tiene

$$x = r \cos\theta, \quad y = r \operatorname{sen} \theta$$

de donde $$z = x + yi = r(\cos\theta + i \operatorname{sen} \theta)$$

El segundo miembro de esta igualdad se llama *forma trigonométrica* (*forma polar*) de z. El número real no negativo

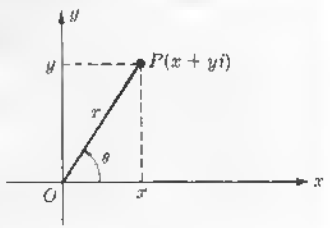


Fig. 8-1.

$$r = |z| = \sqrt{z \cdot \bar{z}} = \sqrt{x^2 + y^2}$$

se llama *módulo* (*valor absoluto*) de z y θ se llama *ángulo* (*amplitud* o *argumento*) de z. Como θ es tal que $x = r\cos\theta$, $y = r\,\text{sen}\,\theta$, $\text{tg}\,\theta = y/x$ y cualesquiera dos de éstos determinan θ dentro de un múltiplo aditivo de 2π. Por lo general se escoge θ como el menor ángulo positivo. (*Nota*. Si P está en O, se tiene $r = 0$ y θ arbitrario.)

Ejemplo 1: Expresar (*a*) $1 + i$, (*b*) $-\sqrt{3} + i$ en forma trigonométrica.

(*a*) Se tiene $r = \sqrt{1+1} = \sqrt{2}$. Como $\text{tg}\,\theta = 1$ y $\cos\theta = 1/\sqrt{2}$, tomamos para θ el ángulo del primer cuadrante $45° = \pi/4$. Así, pues, $1 + i = \sqrt{2}\,(\cos\pi/4 + i\,\text{sen}\,\pi/4)$.

(*b*) Aquí es $r = \sqrt{3+1} = 2$, $\text{tg}\,\theta = -1/\sqrt{3}$ y $\cos\theta = -\frac{1}{2}\sqrt{3}$. Tomando para θ el ángulo del segundo cuadrante $5\pi/6$ se tiene

$$-\sqrt{3} + i = 2(\cos 5\pi/6 + i\,\text{sen}\,5\pi/6)$$

Se sigue que dos números complejos son iguales si, y solo si, sus valores absolutos son iguales y si sus ángulos difieren en un múltiplo entero de 2π, esto es, si son congruentes módulo 2π.

En los Problemas 3 y 4 se demuestran el

Teorema III. El valor absoluto del producto de dos números complejos es el producto de sus valores absolutos y el ángulo del producto es la suma de sus ángulos.

y el

Teorema IV. El valor absoluto del cociente de dos números complejos es el cociente de sus valores absolutos y el ángulo del cociente es el ángulo del numerador menos el ángulo del denominador.

Ejemplo 2: (*a*) Si $z_1 = 2(\cos\frac{1}{4}\pi + i\,\text{sen}\,\frac{1}{4}\pi)$ y $z_2 = 4(\cos\frac{3}{4}\pi + i\,\text{sen}\,\frac{3}{4}\pi)$, se tiene

$$z_1 \cdot z_2 = 2(\cos\tfrac{1}{4}\pi + i\,\text{sen}\,\tfrac{1}{4}\pi)\cdot 4(\cos\tfrac{3}{4}\pi + i\,\text{sen}\,\tfrac{3}{4}\pi)$$
$$= 8(\cos\pi + i\,\text{sen}\,\pi) = -8$$
$$z_2/z_1 = 4(\cos\tfrac{3}{4}\pi + i\,\text{sen}\,\tfrac{3}{4}\pi) : 2(\cos\tfrac{1}{4}\pi + i\,\text{sen}\,\tfrac{1}{4}\pi)$$
$$= 2(\cos\tfrac{1}{2}\pi + i\,\text{sen}\,\tfrac{1}{2}\pi) = 2i$$
$$z_1/z_2 = \tfrac{1}{2}(\cos(-\tfrac{1}{2}\pi) + i\,\text{sen}\,(-\tfrac{1}{2}\pi)) = \tfrac{1}{2}(\cos 3\pi/2 + i\,\text{sen}\,3\pi/2) = -\tfrac{1}{2}i$$

(*b*) Si $z = 2(\cos\pi/6 + i\,\text{sen}\,\pi/6)$,

$$z^2 = z \cdot z = 4(\cos\pi/3 + i\,\text{sen}\,\pi/3) = 2(1 + i\sqrt{3})$$

y

$$z^3 = z^2 \cdot z = 8(\cos\tfrac{1}{2}\pi + i\,\text{sen}\,\tfrac{1}{2}\pi) = 8i$$

Como consecuencia del Teorema IV, se tiene

Teorema V. Si n es un entero positivo

$$[r(\cos\theta + i\,\text{sen}\,\theta)]^n = r^n(\cos n\theta + i\,\text{sen}\,n\theta)$$

Las

ecuación

$$z^n = A = \rho(\cos\phi + i\,\text{sen}\,\phi)$$

n es un entero positivo y A es cualquier número complejo, tiene exactamente n raíces como se verá en seguida. Si $z = r(\cos\theta + i\,\text{sen}\,\theta)$ es una de éstas, se tiene por el Teorema V

$$r^n(\cos n\theta + i\,\text{sen}\,n\theta) = \rho(\cos\phi + i\,\text{sen}\,\phi)$$

$$r^n = \rho \quad \text{y} \quad n\theta = \phi + 2k\pi \quad (k, \text{ entero})$$

$$r = \rho^{1/n} \quad \text{y} \quad \theta = \phi/n + 2k\pi/n$$

El número de raíces distintas es el de ángulos del conjunto $\{\phi/n + 2k\pi/n\}$ que no terminan en el mismo lado. Para cualquier entero positivo $k = nq + m$, $0 \leq m < n$, es claro que $\phi/n + 2k\pi/n$ y $\phi/n + 2m\pi/n$ tienen lados terminales coincidentes. Así, pues, hay exactamente n raíces distintas dadas por

$$\rho^{1/n}[\cos(\phi/n + 2k\pi/n) + i \operatorname{sen}(\phi/n + 2k\pi/n)], \quad k = 0, 1, 2, 3, \ldots, n-1$$

Estas n raíces son coordenadas de n puntos equidistantes sobre el círculo de centro en el origen y de radio $\sqrt[n]{|A|}$. Si entonces $z = \sqrt[n]{|A|}\,(\cos 0 + i \operatorname{sen} 0)$ es cualquiera de las raíces *enésimas* de A, las otras raíces se obtendrán sucesivamente aumentando el ángulo 0 en $2\pi/n$ y reduciendo módulo 2π cuando quiera que el ángulo sea mayor que 2π.

Ejemplo 3: (*a*) Una raíz de $z^4 = 1$ es $r_1 = 1 = \cos 0 + i \operatorname{sen} 0$. Aumentando el ángulo sucesivamente en $2\pi/4 = \pi/2$, se encuentra $r_2 = \cos \frac{1}{2}\pi + i \operatorname{sen} \frac{1}{2}\pi$, $r_3 = \cos \pi + i \operatorname{sen} \pi$ y $r_4 = \cos 3\pi/2 + i \operatorname{sen} 3\pi/2$. Nótese que si hubiéramos comenzado con otra raíz, digamos $-1 = \cos \pi + i \operatorname{sen} \pi$, habríamos obtenido $\cos 3\pi/2 + i \operatorname{sen} 3\pi/2$, $\cos 2\pi + i \operatorname{sen} 2\pi = \cos 0 + i \operatorname{sen} 0$ y $\cos \frac{1}{2}\pi + i \operatorname{sen} \frac{1}{2}\pi$. Estas son, desde luego, las mismas raíces obtenidas antes solo que en orden diferente.

(*b*) Una de las raíces de $z^6 = -4\sqrt{3} - 4i = 8(\cos 7\pi/6 + i \operatorname{sen} 7\pi/6)$ es

$$r_1 = \sqrt{2}\,(\cos 7\pi/36 + i \operatorname{sen} 7\pi/36)$$

Aumentando sucesivamente el ángulo en $2\pi/6$, tenemos

$$r_2 = \sqrt{2}\,(\cos 19\pi/36 + i \operatorname{sen} 19\pi/36)$$

$$r_3 = \sqrt{2}\,(\cos 31\pi/36 + i \operatorname{sen} 31\pi/36)$$

$$r_4 = \sqrt{2}\,(\cos 43\pi/36 + i \operatorname{sen} 43\pi/36)$$

$$r_5 = \sqrt{2}\,(\cos 55\pi/36 + i \operatorname{sen} 55\pi/36)$$

$$r_6 = \sqrt{2}\,(\cos 67\pi/36 + i \operatorname{sen} 67\pi/36)$$

Como consecuencia del Teorema V se tiene el

Teorema VI. Las n raíces *enésimas* de la unidad son

$$\rho = \cos 2\pi/n + i \operatorname{sen} 2\pi/n, \quad \rho^2, \rho^3, \rho^4, \ldots, \rho^{n-1}, \rho^n = 1$$

RAICES PRIMITIVAS DE LA UNIDAD

Una raíz enésima z de 1 se dice *primitiva* si, y solamente si, $z^m \neq 1$ con $0 < m < n$. Mediante los resultados del Problema 5 es fácil mostrar que ρ y ρ^5 son raíces sextas primitivas de 1, en tanto que ρ^2, ρ^3, ρ^4, ρ^6 no lo son. Esto ilustra el

Teorema VII. Sea $\rho = \cos 2\pi/n + i \operatorname{sen} 2\pi/n$. Si $(m, n) = d > 1$, entonces ρ^m es una raíz de orden n/d de 1.

Para una demostración véase Problema 6.

De aquí se sigue el

Corolario. Las raíces n primitivas de 1 son aquellas raíces enésimas, y solo aquellas, $\rho, \rho^2, \rho^3, \ldots, \rho^n$ de 1 cuyos exponentes son primos relativos con n.

Ejemplo 4: Las raíces 12 más primitivas de 1 son

$$\rho = \cos 2\pi/12 + i \operatorname{sen} 2\pi/12 = \tfrac{1}{2}\sqrt{3} + \tfrac{1}{2}i$$

$$\rho^5 = \cos 5\pi/6 + i \operatorname{sen} 5\pi/6 = -\tfrac{1}{2}\sqrt{3} + \tfrac{1}{2}i$$

$$\rho^7 = \cos 7\pi/6 + i \operatorname{sen} 7\pi/6 = -\tfrac{1}{2}\sqrt{3} - \tfrac{1}{2}i$$

$$\rho^{11} = \cos 11\pi/6 + i \operatorname{sen} 11\pi/6 = \tfrac{1}{2}\sqrt{3} - \tfrac{1}{2}i$$

Problemas resueltos

1. Expresar en la forma $x + yi$:

$(a)\ 3 - 2\sqrt{-1}$, $(b)\ 3 + \sqrt{-4}$, $(c)\ 5$, $(d)\ \dfrac{1}{3+4i}$, $(e)\ \dfrac{5-i}{2-3i}$, $(f)\ i^3$.

$(a)\ 3 - 2\sqrt{-1} = 3 - 2i$

$(b)\ 3 + \sqrt{-4} = 3 + 2i$

$(c)\ 5 = 5 + 0 \cdot i$

$(d)\ \dfrac{1}{3+4i} = \dfrac{3-4i}{(3+4i)(3-4i)} = \dfrac{3-4i}{25} = \dfrac{3}{25} - \dfrac{4}{25}i$

$(e)\ \dfrac{5-i}{2-3i} = \dfrac{(5-i)(2+3i)}{(2-3i)(2+3i)} = \dfrac{13+13i}{13} = 1 + i$

$(f)\ i^3 = i^2 \cdot i = -i = 0 - i$

2. Demostrar: La aplicación $z \leftrightarrow \bar{z}$, $z \in C$ es un isomorfismo de C sobre C.

Vamos a demostrar que la adición y la multiplicación se preservan en la aplicación. Lo cual se sigue de que siendo para

$$z_1 = x_1 + y_1 i,\quad z_2 = x_2 + y_2 i \in C,$$

$$\overline{z_1 + z_2} = \overline{(x_1 + y_1 i) + (x_2 + y_2 i)} = \overline{(x_1 + x_2) + (y_1 + y_2)i}$$
$$= (x_1 + x_2) - (y_1 + y_2)i = (x_1 - y_1 i) + (x_2 - y_2 i) = \bar{z}_1 + \bar{z}_2$$

y

$$\overline{z_1 \cdot z_2} = \overline{(x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i} = (x_1 x_2 - y_1 y_2) - (x_1 y_2 + x_2 y_1)i$$
$$= (x_1 - y_1 i) \cdot (x_2 - y_2 i) = \bar{z}_1 \cdot \bar{z}_2$$

3. Demostrar: El valor absoluto del producto de dos números complejos es el producto de sus valores absolutos y el ángulo del producto es la suma de sus ángulos.

Sean $z_1 = r_1(\cos\theta_1 + i \operatorname{sen}\theta_1)$ y $z_2 = r_2(\cos\theta_2 + i \operatorname{sen}\theta_2)$. Entonces

$$z_1 \cdot z_2 = r_1 r_2[(\cos\theta_1 \cdot \cos\theta_2 - \operatorname{sen}\theta_1 \cdot \operatorname{sen}\theta_2) + i(\operatorname{sen}\theta_1 \cdot \cos\theta_2 + \operatorname{sen}\theta_2 \cdot \cos\theta_1)]$$
$$= r_1 r_2[\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2)]$$

4. Demostrar: El valor absoluto del cociente de dos números complejos es el cociente de sus valores absolutos y el ángulo del cociente es el ángulo del numerador menos el ángulo del denominador.

Para los números complejos z_1 y z_2 del Problema 3,

$$\frac{z_1}{z_2} = \frac{r_1(\cos\theta_1 + i \operatorname{sen}\theta_1)}{r_2(\cos\theta_2 + i \operatorname{sen}\theta_2)} = \frac{r_1(\cos\theta_1 + i \operatorname{sen}\theta_1)(\cos\theta_2 - i \operatorname{sen}\theta_2)}{r_2(\cos\theta_2 + i \operatorname{sen}\theta_2)(\cos\theta_2 - i \operatorname{sen}\theta_2)}$$
$$= \frac{r_1}{r_2}[(\cos\theta_1 \cos\theta_2 + \operatorname{sen}\theta_1 \operatorname{sen}\theta_2) + i(\operatorname{sen}\theta_1 \cos\theta_2 - \operatorname{sen}\theta_2 \cos\theta_1)]$$
$$= \frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i \operatorname{sen}(\theta_1 - \theta_2)]$$

5. Hallar las 6 raíces sextas de 1 y demostrar que entre ellas están las raíces cuadradas y las raíces cúbicas de 1.

Las raíces sextas de 1 son

$$\rho = \cos\pi/3 + i \operatorname{sen}\pi/3 = \tfrac{1}{2} + \tfrac{1}{2}\sqrt{3}\,i \qquad \rho^4 = \cos 4\pi/3 + i \operatorname{sen} 4\pi/3 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{3}\,i$$
$$\rho^2 = \cos 2\pi/3 + i \operatorname{sen} 2\pi/3 = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{3}\,i \qquad \rho^5 = \cos 5\pi/3 + i \operatorname{sen} 5\pi/3 = \tfrac{1}{2} - \tfrac{1}{2}\sqrt{3}\,i$$
$$\rho^3 = \cos\pi + i \operatorname{sen}\pi = -1 \qquad \rho^6 = \cos 2\pi + i \operatorname{sen} 2\pi = 1$$

De éstas, $\rho^3 = -1$ y $\rho^6 = 1$ son raíces cuadradas de 1 y $\rho^2 = -\frac{1}{2} + \frac{1}{2}\sqrt{3}\,i$, $\rho^4 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}\,i$, y $\rho^6 = 1$ son raíces cúbicas de 1.

6. Demostrar: Sea $\rho = \cos 2\pi/n + i \operatorname{sen} 2\pi/n$. Si $(m, n) = d > 1$, entonces ρ^m es una raiz de orden n/d de 1.

Sean $m = m_1 d$ y $n = n_1 d$. Como $\rho^m = \cos 2m\pi/n + i \operatorname{sen} 2m\pi/n = \cos 2m_1\pi/n_1 + i \operatorname{sen} 2m_1\pi/n_1$ y $(\rho^m)^{n_1} = \cos 2m_1\pi + i \operatorname{sen} 2m_1\pi = 1$, se sigue que ρ^m es una raiz $n_1 = n/d$-ésima de 1.

Problemas propuestos

7. Expresar los siguientes números en la forma $x+yi$: (*a*) $2 + \sqrt{-5}$, (*b*) $(4 + \sqrt{-5}) + (3 - 2\sqrt{-5})$, (*c*) $(4 + \sqrt{-5}) - (3 - 2\sqrt{-5})$, (*d*) $(3 + 4i) \cdot (4 - 5i)$, (*e*) $\dfrac{1}{2 - 3i}$, (*f*) $\dfrac{2 + 3i}{5 - 2i}$, (*g*) $\dfrac{5 - 2i}{2 + 3i}$, (*h*) i^4, (*i*) i^5, (*j*) i^6, (*k*) i^8.

Resp. (*a*) $2 + \sqrt{5}\,i$, (*b*) $7 - \sqrt{5}\,i$, (*c*) $1 + 3\sqrt{5}\,i$, (*d*) $32 + i$, (*e*) $2/13 + 3i/13$, (*f*) $4/29 + 19i/29$, (*g*) $4/13 - 19i/13$, (*h*) $1 + 0 \cdot i$, (*i*) $0 + i$, (*j*) $-1 + 0 \cdot i$, (*k*) $1 + 0 \cdot i$

8. Dar los conjugados de: (*a*) $2 + 3i$, (*b*) $2 - 3i$, (*c*) 5, (*d*) $2i$.
Resp. (*a*) $2 - 3i$, (*b*) $2 + 3i$, (*c*) 5, (*d*) $-2i$

9. Demostrar: El conjugado del conjugado de z es z mismo.

10. Demostrar: Para todo $z \neq 0 \in C$, $\overline{(z^{-1})} = (\bar{z})^{-1}$.

11. Situar todos los puntos cuyas coordenadas son de la forma (*a*) $(a + 0 \cdot i)$, (*b*) $(0 + bi)$ donde $a, b \in R$. Demuéstrese que cada punto z y su conjugado son simétricos respecto del eje x.

12. Expresar en forma trigonométrica:

(*a*) 5 (*c*) $-1 - \sqrt{3}\,i$ (*e*) -6 (*g*) $-3 + \sqrt{3}\,i$ (*i*) $1/i$

(*b*) $4 - 4i$ (*d*) $-3i$ (*f*) $\sqrt{2} + \sqrt{2}\,i$ (*h*) $-1/(1 + i)$

Rrsp. (*a*) $5 \operatorname{cis} 0$ (*d*) $3 \operatorname{cis} 3\pi/2$ (*g*) $2\sqrt{3} \operatorname{cis} 5\pi/6$

(*b*) $4\sqrt{2} \operatorname{cis} 7\pi/4$ (*e*) $6 \operatorname{cis} \pi$ (*h*) $\sqrt{2}/2 \operatorname{cis} 3\pi/4$

(*c*) $2 \operatorname{cis} 4\pi/3$ (*f*) $2 \operatorname{cis} \pi/4$ (*i*) $\operatorname{cis} 3\pi/2$

siendo $\operatorname{cis}\theta = \cos\theta + i \operatorname{sen}\theta$.

13. Expresar en la forma $a + bi$:

(*a*) $5 \operatorname{cis} 60°$ (*e*) $(2 \operatorname{cis} 25°) \cdot (3 \operatorname{cis} 335°)$

(*b*) $2 \operatorname{cis} 90°$ (*f*) $(10 \operatorname{cis} 100°) \cdot (\operatorname{cis} 140°)$

(*c*) $\operatorname{cis} 150°$ (*g*) $(6 \operatorname{cis} 170°) : (3 \operatorname{cis} 50°)$

(*d*) $2 \operatorname{cis} 210°$ (*h*) $(4 \operatorname{cis} 20°) : (8 \operatorname{cis} 80°)$

Resp. (*a*) $5/2 + 5\sqrt{3}\,i/2$ (*e*) $-\frac{1}{2}\sqrt{3} + \frac{1}{2}i$ (*e*) 6 (*g*) $-1 + \sqrt{3}\,i$

(*b*) $2i$ (*d*) $-\sqrt{3} - i$ (*f*) $-5 - 5\sqrt{3}\,i$ (*h*) $\frac{1}{4} - \frac{1}{4}\sqrt{3}\,i$

14. Hallar las raices cúbicas de: (*a*) 1, (*b*) 8, (*c*) $27i$, (*d*) $-8i$, (*e*) $-4\sqrt{3} - 4i$.

Resp. (*a*) $-\frac{1}{2} \pm \frac{1}{2}\sqrt{3}\,i$, 1; (*b*) $-1 \pm \sqrt{3}\,i$, 2; (*c*) $\pm\dfrac{3\sqrt{3}}{2} + \dfrac{3}{2}i$, $-3i$; (*d*) $2i$, $\pm\sqrt{3} - i$; (*e*) $2 \operatorname{cis} 7\pi/18$, $2 \operatorname{cis} 19\pi/18$, $2 \operatorname{cis} 31\pi/18$

15. Hallar (*a*) las raices quintas primitivas de 1, (*b*) las raices octavas primitivas de i.

16. Demostrar: La suma de las n raices enésimas distintas de 1 es cero.

17. Utilizando la Fig. 8-2 demostrar:

(*a*) $|z_1 + z_2| \leq |z_1| + |z_2|$

(*b*) $|z_1 - z_2| \geq |z_1| - |z_2|$

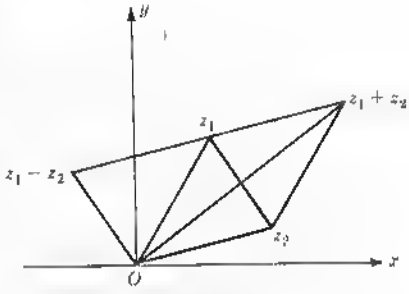


Fig. 8-2.

18. Si r es una raiz cúbica cualquiera de $a \in C$, entonces $r, \omega r, \omega^2 r$ donde $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{3}\,i$ y ω^2 son las raices cúbicas imaginarias de 1, son las tres raices cúbicas de a.

19. Describir geométricamente las aplicaciones

(*a*) $z \to \bar{z}$ (*b*) $z \to zi$ (*c*) $z \to \bar{z}i$

20. Sea en el plano real K el círculo con centro en 0 y radio 1 y sea $A_1A_2A_3$, donde $A_j(x_j, y_j) = A_j(z_j) = A_j(x_j + y_j i)$, $j = 1, 2, 3$, es un triángulo inscrito. Denótese por $P(z) = P(x + yi)$ un punto cualquiera variable del plano.

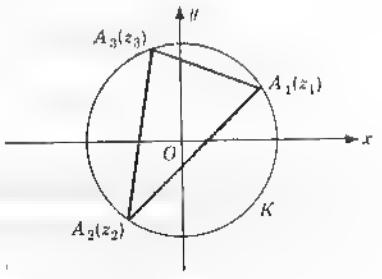


Fig. 8-3.

(*a*) Encontrar que la ecuación de K es $z \cdot \bar{z} = 1$.

(*b*) Demostrar que $P_r(x_r, y_r)$ donde $x_r = \dfrac{ax_j + bx_k}{a+b}$ y $y_r = \dfrac{ay_j + by_k}{a+b}$, divide el segmento A_j, A_k en la razón $b : a$. Luego, como A_j, A_k y $P_r\left(\dfrac{az_j + bz_k}{a+b}\right)$ están en la recta A_j, A_k, comprobar que la ecuación de ésta es $z + z_j z_k \bar{z} = z_j + z_k$.

(*c*) Comprobar: La ecuación de toda paralela a A_jA_k tiene la forma $z + z_j z_k \bar{z} = \eta$ demostrando que los puntos medios B_j y B_k de A_iA_j y A_iA_k están sobre la recta $z + z_j z_k \bar{z} = \frac{1}{2}(z_i + z_j + z_k + z_i z_j z_k)$.

(*d*) Comprobar: La ecuación de toda recta perpendicular a A_jA_k tiene la forma $z - z_j z_k \bar{z} = \mu$ demostrando que 0 y el punto medio de A_jA_k están sobre la recta $z - z_j z_k \bar{z} = 0$.

(*e*) Utilizar $z = z_i$ en $z - z_j z_k \bar{z} = \mu$ para obtener la ecuación $z - z_j z_k \bar{z} = \bar{z}_i - z_i z_j z_k$ de la altura por A_i de $A_1A_2A_3$. Luego eliminar $\bar{z}$ entre las ecuaciones de dos alturas cualesquiera para obtener su punto de intersección $H(z_1 + z_2 + z_3)$. Demuéstrese que H también está en la tercera altura.

Capítulo 9

Grupos

GRUPOS

Un conjunto no vacío $\mathscr{G}$ sobre el cual se ha definido una operación binaria $\circ$ se llama grupo con respecto a esta operación si para cualesquiera $a, b, c \in \mathscr{G}$ se verifican las propiedades siguientes:

$\mathbf{P}_1$: $(a \circ b) \circ c = a \circ (b \circ c)$ (ley asociativa)

$\mathbf{P}_2$: Existe un $u \in \mathscr{G}$ tal que $a \circ u = u \circ a = a$ (existencia de elemento neutro)

$\mathbf{P}_3$: Para cada $a \in \mathscr{G}$ existe un $a^{-1} \in \mathscr{G}$ tal que $a \circ a^{-1} = a^{-1} \circ a = u$ (existencia del simétrico)

Nota 1. No ha de haber lugar a confusión por el empleo en $\mathbf{P}_3$ de a^{-1} para denotar el simétrico de a respecto de la operación $\circ$. La notación ha sido simplemente sacada de la que se utilizó antes para la multiplicación. Cuando la operación del grupo es la adición se ha de interpretar a^{-1} como el simétrico aditivo $-a$.

Nota 2. Los capítulos precedentes contienen muchos ejemplos de grupos para la mayoría de los cuales la operación de grupo es conmutativa. Es de notar aquí que el hecho de que la operación sea conmutativa no se requiere en las propiedades enumeradas arriba. Si la operación es conmutativa, el grupo se dice *abeliano*, pero por el momento no haremos distinción entre grupos abelianos o no abelianos.

Ejemplo 1: (*a*) El conjunto Z de los enteros forma un grupo con respecto a la adición; el elemento neutro es el 0 y el simétrico de $a \in Z$ es el $-a$ o sea, el opuesto de a. Así que en lo sucesivo podemos hablar del grupo aditivo Z. Por otra parte, Z no es grupo multiplicativo, ya que, por ejemplo, ni 0 ni 2 tienen simétricos multiplicativos.

(*b*) El conjunto A del Ejemplo 12(*c*), Capítulo 2, es un grupo con respecto a $\circ$. El elemento neutro es a. Averigüese el simétrico de cada elemento.

(*c*) El conjunto $A = \{-3, -2, -1, 0, 1, 2, 3\}$ no es grupo con respecto a la adición sobre Z si bien 0 es elemento neutro, cada elemento de A tiene simétrico y la adición es asociativa. La razón es, naturalmente, que la adición no es operación binaria sobre A, es decir, que el conjunto A no es cerrado con respecto a la adición.

(*d*) El conjunto $A = \{\omega_1 = -\frac{1}{2} + \frac{1}{2}\sqrt{3}\,i,\ \omega_2 = -\frac{1}{2} - \frac{1}{2}\sqrt{3}\,i,\ \omega_3 = 1\}$ de las raíces cúbicas de 1 forma grupo con respecto a la multiplicación en el conjunto de los números complejos C ya que (i) el producto de dos elementos cualesquiera del conjunto es un elemento del mismo, (ii) se cumple la ley asociativa en C y, por tanto, en A, (iii) ω_3 es el elemento neutro y (iv) los simétricos de $\omega_1, \omega_2, \omega_3$ son, respectivamente, $\omega_2, \omega_1, \omega_3$.

Esto es también evidente por (ii) y la tabla de operación adjunta.

$\cdot$	ω_1	ω_2	ω_3
ω_1	ω_2	ω_3	ω_1
ω_2	ω_3	ω_1	ω_2
ω_3	ω_1	ω_2	ω_3

Tabla 9-1

Véanse también Problemas 1-2.

PROPIEDADES SENCILLAS DE LOS GRUPOS

La unicidad del elemento neutro y del simétrico de cada elemento del grupo fueron demostradas en los Teoremas III y IV, Capítulo 2, página 20. Se deduce fácilmente

Teoremas I. (ley de cancelación). Si $a, b, c \in \mathscr{G}$, de $a \circ b = a \circ c$ (también a $b \circ a = c \circ a$) se sigue $b = c$.

Para demostración, véase Problema 3.

Teorema II. Con $a, b \in \mathscr{G}$, cada una de las ecuaciones $a \circ x = b$ y $y \circ a = b$ tiene una solución única.

Para demostración, véase Problema 4.

Teorema III. Para todo $a \in \mathscr{G}$, el simétrico del simétrico de a es a, es decir, $(a^{-1})^{-1} = a$.

Teorema IV. Para cualesquiera $a, b \in \mathscr{G}$, $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Teorema V. Para cualesquiera $a, b, \ldots, p, q \in \mathscr{G}$, es $(a \circ b \circ \cdots \circ p \circ q)^{-1} = q^{-1} \circ p^{-1} \circ \cdots \circ b^{-1} \circ a^{-1}$.

Para cualquier $a \in \mathscr{G}$ y cualquier $m \in Z^+$, se define

$$a^m = a \circ a \circ a \circ \cdots \circ a \qquad \text{de } m \text{ factores}$$
$$a^0 = u, \text{ el elemento neutro de } \mathscr{G}$$
$$a^{-m} = (a^{-1})^m = a^{-1} \circ a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1} \qquad \text{de } m \text{ factores}$$

De nuevo se ha tomado la notación de la utilizada cuando la operación es la multiplicación. Si la operación es la adición, a^n con $n > 0$ se ha de interpretar como $na = a + a + a + \cdots + a$ con n términos, a^0 como u y a^{-n} como $n(-a) = -a + (-a) + (-a) + \cdots + (-a)$ con n términos. Obsérvese que na es simplemente, pues, una abreviatura y no se ha de considerar como producto de $n \in Z$ por $a \in \mathscr{G}$.

En el Problema 5 se demuestra la primera parte del

Teorema VI. Para todo $a \in \mathscr{G}$, (i) $a^m \circ a^n = a^{m+n}$ y (ii) $(a^m)^n = a^{mn}$, con $m, n \in Z$.

Se entiende por *orden de un grupo* $\mathscr{G}$ el número de elementos del conjunto $\mathscr{G}$. El grupo aditivo Z del Ejemplo 1(a) es de orden infinito; los grupos del Ejemplo 1(b) y 1(d) son grupos finitos de orden 5 y de orden 3, respectivamente.

Por *orden de un elemento* $a \in \mathscr{G}$ se entiende el menor entero positivo n, si existe, para el cual $a^n = u$, el elemento neutro de $\mathscr{G}$. Si $a \neq 0$ es un elemento del grupo aditivo Z, entonces, puesto que $na \neq 0$ para todo entero positivo n, el orden de a es infinito. El elemento ω_1 del Ejemplo 1(d) es de orden 3, pues ω_1 y ω_1^2 son diferentes de 1 mientras que $\omega_1^3 = 1$, el elemento neutro.

SUBGRUPOS

Sea $\mathscr{G} = \{a, b, c, \ldots\}$ un grupo respecto de $\circ$. Cualquier subconjunto no vacío $\mathscr{G}'$ de $\mathscr{G}$ se llama *subgrupo* de $\mathscr{G}$ si $\mathscr{G}'$ es él mismo un grupo con respecto a $\circ$. Evidentemente $\mathscr{G}' = \{u\}$, donde u es el elemento neutro de $\mathscr{G}$ y $\mathscr{G}$ mismo, son subgrupos de cualquier grupo $\mathscr{G}$. Se les llamará subgrupos *impropios*; otros subgrupos de $\mathscr{G}$, si los hay, se llamarán *propios*. Es de notar de paso que todo subgrupo de un grupo $\mathscr{G}$ contiene a u como elemento neutro.

Ejemplo 2: (a) Un subgrupo propio del grupo multiplicativo $\mathscr{G} = \{1, -1, i, -i\}$ es $\mathscr{G}' = \{1, -1\}$. (¿Hay otros?)

(b) Considérese el grupo multiplicativo $\mathscr{G} = \{\rho, \rho^2, \rho^3, \rho^4, \rho^5, \rho^6 = 1\}$ de las raíces sextas de la unidad (véase Problema 5, Capítulo 8, página 79). Tiene como subgrupos propios $\mathscr{G}' = \{\rho^3, \rho^6\}$ y $\mathscr{G}'' = \{\rho^2, \rho^4, \rho^6\}$.

Los dos siguientes teoremas son útiles para determinar cuándo un subconjunto de un grupo $\mathscr{G}$ de operación de grupo $\circ$ es o no subgrupo del $\mathscr{G}$.

Teorema VII. Un subconjunto $\mathscr{G}'$ no vacio de un grupo $\mathscr{G}$ es subgrupo de $\mathscr{G}$ si, y solamente si, (i) $\mathscr{G}'$ es cerrado con respecto a $\circ$, (ii) $\mathscr{G}'$ contiene el simètrico de cada uno de sus elementos.

Teorema VIII. Un subconjunto $\mathscr{G}'$ no vacio de un grupo $\mathscr{G}$ es subgrupo de $\mathscr{G}$ si, y solamente si, para cualesquiera $a, b \in \mathscr{G}'$, $a^{-1} \circ b \in \mathscr{G}'$.

Para demostración, vèase Problema 6.

De lo que se sigue el

Teorema IX. Sea a un elemento de un grupo $\mathscr{G}$. El conjunto $\mathscr{G}' = \{a^n : n \in Z\}$ de todas las potencias enteras de a es un subgrupo de $\mathscr{G}$.

Teorema X. Si S es cualquier conjunto de subgrupos de un grupo $\mathscr{G}$, la intersección de estos subgrupos es también un subgrupo de $\mathscr{G}$.

Para demostración, vèase Problema 7.

GRUPOS CICLICOS

Un grupo $\mathscr{G}$ se dice *cíclico* si, para algún $a \in \mathscr{G}$, todo $x \in \mathscr{G}$ es de la forma a^m, donde $m \in Z$. El elemento a se llama entonces un *generador* de $\mathscr{G}$. Evidentemente, todo grupo cíclico es abeliano.

Ejemplo 3:

(*a*) El grupo aditivo Z es cíclico con generador $a = 1$, pues para todo $m \in Z$, $a^m = ma = m$.

(*b*) El grupo multiplicativo de las raíces quintas de 1 es cíclico. A diferencia del grupo de (*a*), que solo tiene 1 y -1 como generadores, este grupo puede ser generado por cualquiera de sus elementos excepto el 1.

(*c*) El grupo $\mathscr{G}$ del Ejemplo 2(*b*) es cíclico. Sus generadores son ρ y ρ^5.

Los Ejemplos 3(*b*) y 3(*c*) ilustran el

Teorema XI. Un elemento a^t de un grupo cíclico finito $\mathscr{G}$ de orden n es un generador de $\mathscr{G}$ si, y solo si $(n, t) = 1$.

En el Problema 8 se demuestra el

Teorema XII. Todo subgrupo de un grupo cíclico es él mismo un grupo cíclico.

GRUPOS DE PERMUTACIONES

En el Capítulo 2 se estudió el conjunto S_n de las $n!$ permutaciones de n símbolos. Este conjunto resulta ser un grupo con respecto a la operación de permutación $\circ$. Como $\circ$ no es conmutativa, éste es nuestro primer ejemplo de un grupo no abeliano.

Es costumbre llamar al grupo S_n *grupo simètrico* de n símbolos y a cualquier subgrupo de S_n *grupo de permutación* de n símbolos.

Ejemplo 4:

(*a*) $S_4 = \{(1), (12), (13), (14), (23), (24), (34), \alpha = (123), \alpha^2 = (132), \beta = (124), \beta^2 = (142), \gamma = (134), \gamma^2 = (143), \delta = (234), \delta^2 = (243), \rho = (1234), \rho^2 = (13)(24), \rho^3 = (1432), \sigma = (1243), \sigma^2 = (14)(23), \sigma^3 = (1342), \tau = (1324), \tau^2 = (12)(34), \tau^3 = (1423)\}$.

(*b*) Los subgrupos de S_4: (i) $\{(1), (12)\}$, (ii) $\{(1), \alpha, \alpha^2\}$, (iii) $\{(1), (12), (34), (12)(34)\}$, y (iv) $A_4 = \{(1), \alpha, \alpha^2, \beta, \beta^2, \gamma, \gamma^2, \delta, \delta^2, \rho^2, \sigma^2, \tau^2\}$, son ejemplos de grupos de permutación de 4 símbolos. (A_4 consiste en todas las permutaciones pares de S_4 y se le conoce como *grupo alternante* de 4 símbolos. ¿Cuáles de los anteriores subgrupos son cíclicos? ¿cuáles abelianos? Dar otros subgrupos de S_4.

Véanse Problemas 9-10.

HOMOMORFISMOS

Sean dos grupos, $\mathscr{G}$ con la operación $\circ$, y $\mathscr{G}'$ con la operación $\square$. Se llama *homomorfismo* de $\mathscr{G}$ en $\mathscr{G}'$ una aplicación

$$\mathscr{G} \to \mathscr{G}' : g \to g'$$

tal que

(i) todo $g \in \mathcal{G}$ tiene una imagen única $g' \in \mathcal{G}'$
(ii) si $a \to a'$ y $b \to b'$, entonces $a \circ b \to a' \square b'$

Si además la aplicación es sobreyectiva, esto es, si

(iii) todo $g' \in \mathcal{G}'$ es imagen

se tiene un homomorfismo de $\mathcal{G}$ *sobre* $\mathcal{G}'$ y se dirá que $\mathcal{G}'$ es una *imagen homomorfa* de $\mathcal{G}$.

Ejemplo 5: (*a*) Sea la aplicación $n \to i^n$ del grupo aditivo Z sobre el grupo multiplicativo de las raíces cuartas de 1. Es un homomorfismo, puesto que

$$m + n \to i^{m+n} = i^m \cdot i^n$$

y se preservan las operaciones de grupo.

(*b*) Sean el grupo cíclico $\mathcal{G} = \{a, a^2, a^3, \ldots, a^{12} = u\}$ y su subgrupo $\mathcal{G}' = \{a^2, a^4, a^6, \ldots, a^{12}\}$. Se ve fácilmente que la aplicación

$$a^n \to a^{2n}$$

es un homomorfismo de $\mathcal{G}$ sobre $\mathcal{G}'$ en tanto que la aplicación

$$a^n \to a^n$$

es un homomorfismo de $\mathcal{G}'$ en $\mathcal{G}$ simplemente.

Véase Problema 11.

En el Problema 12 se demuestra el

Teorema XIII. En cualquier homomorfismo entre dos grupos $\mathcal{G}$ y $\mathcal{G}'$ los elementos neutros se corresponden, y si $x \in \mathcal{G}$ y $x' \in \mathcal{G}'$ se corresponden, lo mismo ocurre con sus simétricos.

Se sigue de esto que

Teorema XIV. La imagen homomorfa de todo grupo cíclico es cíclica.

ISOMORFISMOS

Si la aplicación de la sección anterior es biyectiva, es decir, si

$$g \leftrightarrow g'$$

se dice que $\mathcal{G}$ y $\mathcal{G}'$ son *isomorfos* y la aplicación se llama *isomorfismo*.

Ejemplo 6: Mostrar que $\mathcal{G}$, el grupo aditivo $Z/(4)$ es isomorfo a $\mathcal{G}'$, el grupo multiplicativo de elementos no nulos de $Z/(5)$.

Examínense las tablas de operación.

$\mathcal{G}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabla 9-2

$\mathcal{G}'$

·	1	3	4	2
1	1	3	4	2
3	3	4	2	1
4	4	2	1	3
2	2	1	3	4

Tabla 9-3

en las que por comodidad se han remplazado [0], [1], . . . , por 0, 1, . . . Se ve claramente que la aplicación

$$\mathcal{G} \to \mathcal{G}' : 0 \to 1,\ 1 \to 3,\ 2 \to 4,\ 3 \to 2$$

es un isomorfismo. Por ejemplo, $1 = 2 + 3 \to 4 \cdot 2 = 3$, etc.

Rehacer la tabla de operación de $\mathcal{G}'$ para mostrar que

$$\mathcal{G} \to \mathcal{G}' : 0 \to 1,\ 1 \to 2,\ 2 \to 4,\ 3 \to 3$$

es otro isomorfismo de $\mathcal{G}$ sobre $\mathcal{G}'$. ¿Hay otro?

En el Problema 13 se demuestra la primera parte del

Teorema XV. (*a*) Todo grupo cíclico de orden infinito es isomorfo al grupo aditivo Z.

(*b*) Todo grupo cíclico de orden finito n es isomorfo al grupo aditivo $Z/(n)$.

El resultado más notable de esta sección es el

Teorema XVI (Cayley). Todo grupo finito de orden n es isomorfo a un grupo de permutación de n símbolos.

Como la demostración, que se da en el Problema 14, consiste en ver cómo se construye de hecho un grupo de permutación, el lector querrá examinar ante todo el

Ejemplo 7: Considérese la tabla de operación adjunta para el grupo $\mathcal{G} = \{g_1, g_2, g_3, g_4, g_5, g_6\}$ con la operación de grupo $\square$.

$\square$	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_1	g_2	g_3	g_4	g_5	g_6
g_2	g_2	g_1	g_5	g_6	g_3	g_4
g_3	g_3	g_6	g_1	g_5	g_4	g_2
g_4	g_4	g_5	g_6	g_1	g_2	g_3
g_5	g_5	g_4	g_2	g_3	g_6	g_1
g_6	g_6	g_3	g_4	g_2	g_1	g_5

Tabla 9-4

Los elementos de cualquier columna de la tabla, digamos la quinta: $g_1 \square g_5 = g_5, g_2 \square g_5 = g_3, g_3 \square g_5 = g_4, g_4 \square g_5 = g_2, g_5 \square g_5 = g_6, g_6 \square g_5 = g_1$ son los elementos de la fila de encabezamientos (o sea los elementos del grupo $\mathcal{G}$) en otro orden. Esta permutación se indicará por

$$\begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 \\ g_3 & g_6 & g_4 & g_2 & g_5 & g_1 \end{pmatrix} = (156)(234) = p_5$$

Se sigue fácilmente que $\mathcal{G}$ es isomorfo a $P = \{p_1, p_2, p_3, p_4, p_5, p_6\}$ donde $p_1 = (1)$, $p_2 = (12)(36)(45)$, $p_3 = (13)(25)(46)$, $p_4 = (14)(26)(35)$, $p_5 = (156)(234)$, $p_6 = (165)(243)$ por la aplicación

$$g_i \leftrightarrow p_i \qquad (i = 1, 2, 3, \ldots, 6)$$

CLASES LATERALES SEGUN UN SUBGRUPO

Sea $\mathcal{G}$ un grupo finito con la operación de grupo $\circ$; sean H un subgrupo de $\mathcal{G}$ y a un elemento cualquiera de $\mathcal{G}$. Se llama *clase a la derecha según el subgrupo* H de $\mathcal{G}$, generada por a al subconjunto Ha de $\mathcal{G}$

$$Ha = \{h \circ a : h \in H\}$$

y *clase a la izquierda según el subgrupo* H de $\mathcal{G}$, generada por a, al subconjunto aH de $\mathcal{G}$

$$aH = \{a \circ h : h \in H\}$$

Ejemplo 8: El subgrupo $H = \{(1), (12), (34), (12)(34)\}$ y el elemento $a = (1432)$ de S_4 generan la clase a la derecha

$$\begin{aligned} Ha &= \{(1) \circ (1432), (12) \circ (1432), (34) \circ (1432), (12)(34) \circ (1432)\} \\ &= \{(1432), (243), (142), (24)\} \end{aligned}$$

y la clase a la izquierda

$$\begin{aligned} aH &= \{(1432) \circ (1), (1432) \circ (12), (1432) \circ (34), (1432) \circ (12)(34)\} \\ &= \{(1432), (143), (132), (13)\} \end{aligned}$$

Al examinar las propiedades de las clases laterales, por lo general nos limitaremos a las clases a la derecha y dejamos al cuidado del lector el formular las propiedades correspondientes de las clases a la izquierda. Lo primero, nótese que $a \in Ha$ puesto que u, el elemento neutro de $\mathcal{G}$, es también el elemento neutro de H. Si H contiene m elementos, también los contiene Ha, pues Ha contiene a lo más m y $h_1 \circ a = h_2 \circ a$ para cualesquiera $h_1, h_2 \in H$ implica $h_1 = h_2$. Por último, si C_r designa el conjunto de todas las clases a la derecha diferentes según H en $\mathcal{G}$, entonces $H \in C_r$ porque $Ha = H$ cuando $a \in H$.

Considérense ahora dos clases a la derecha Ha y Hb, $a \neq b$ según H en $\mathcal{G}$. Supóngase que c es un elemento común de estas clases de modo que para algunos $h_1, h_2 \in H$ se tiene $c = h_1 \circ a = h_2 \circ b$. Entonces, $a = h_1^{-1} \circ (h_2 \circ b) = (h_1^{-1} \circ h_2) \circ b$ y como $h_1^{-1} \circ h_2 \in H$ (Teorema VIII), se sigue que $a \in Hb$ y que $Ha = Hb$. Así, pues, C_r consiste en clases a la derecha, de $\mathcal{G}$, mutuamente disjuntas y, por tanto, es una partición de $\mathcal{G}$. Se dirá que C_r es una *descomposición* de $\mathcal{G}$ en clases a la derecha según el subgrupo H.

Ejemplo 9: (*a*) Sea $\mathcal{G} = Z$ el grupo aditivo de los enteros y H el subgrupo de los enteros divisibles por 5. La descomposición de $\mathcal{G}$ en clases a la derecha según H consta de las cinco clases residuales módulo 5, esto es, $H = \{x: 5 \mid x\}$, $H1 = \{x: 5 \mid (x-1)\}$, $H2 = \{x: 5 \mid (x-2)\}$, $H3 = \{x: 5 \mid (x-3)\}$, y $H4 = \{x: 5 \mid (x-4)\}$. No hay que distinguir entre clases a la derecha y clases a la izquierda puesto que $\mathcal{G}$ es grupo abeliano.

(*b*) Sean $\mathcal{G} = S_4$ y $H = A_4$ el subgrupo de las permutaciones pares de S_4. Entonces hay solamente dos clases a la derecha (izquierda) de $\mathcal{G}$ respecto de H, a saber, A_4 y el conjunto de las permutaciones impares de S_4. Aquí tampoco hay distinción entre clases a la derecha y a la izquierda, pero nótese que S_4 no es abeliano.

(*c*) Sean $\mathcal{G} = S_4$ y H el grupo octal del Problema 9. Las diferentes clases a la derecha según H, son

$$\begin{aligned} H &= \{(1), (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\} \\ H(12) &= \{(12), (234), (1324), (1431), (34), (1423), (132), (124)\} \\ H(23) &= \{(23), (134), (1243), (142), (1342), (14), (123), (243)\} \end{aligned}$$

y las diferentes clases a la izquierda según H, son

$$\begin{aligned} H &= \{(1), (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\} \\ (12)H &= \{(12), (134), (1423), (243), (34), (1324), (123), (142)\} \\ (23)H &= \{(23), (124), (1342), (143), (1243), (14), (132), (234)\} \end{aligned}$$

Así, pues, $G = H \cup H(12) \cup H(23) = H \cup (12)H \cup (23)H$. Aquí la descomposición de $\mathcal{G}$ es diferente según se utilicen las clases a la derecha o las clases a la izquierda, según H.

Sea $\mathcal{G}$ un grupo finito de orden n y sea H un subgrupo de $\mathcal{G}$ de orden m. El número de clases diferentes a la derecha según H en $\mathcal{G}$ (llamado *índice* de H en $\mathcal{G}$) es r con $n = mr$; por consiguiente:

Teorema XVII (Lagrange). El orden de cada subgrupo de un grupo finito $\mathcal{G}$ es divisor del orden de $\mathcal{G}$.

Como consecuencia, se tienen los

Teorema XVIII. Si $\mathcal{G}$ es un grupo finito de orden n, entonces el orden de cualquier elemento $a \in \mathcal{G}$ (es decir, el orden del subgrupo cíclico generado por a) es divisor de n.

y

Teorema XIX. Todo grupo de orden primo es cíclico.

SUBGRUPOS INVARIANTES

Un subgrupo H de un grupo $\mathcal{G}$ se llama *subgrupo invariante* (también *subgrupo distinguido*, *subgrupo normal* o *divisor normal*) de $\mathcal{G}$ si

(i) $$gH = Hg \qquad \text{para todo } g \in \mathcal{G}$$

Como $g^{-1} \in \mathcal{G}$ si $g \in \mathcal{G}$, (i) se puede remplazar por

(i') $$g^{-1}Hg = H \qquad \text{para todo } g \in \mathcal{G}$$

Pero (i') requiere que

(i_1') para todo $g \in \mathcal{G}$ y cualquier $h \in H$, $g^{-1} \circ h \circ g \in H$

y que

(i_2') para todo $g \in \mathcal{G}$ y cada $h \in H$, existe algún $k \in H$ tal que $g^{-1} \circ k \circ g = h$ o bien $k \circ g = g \circ h$.

Se demuestra que (i_1') implica (i_2'). Considérese cualquier $h \in H$. Por (i_1'), $(g^{-1})^{-1} \circ h \circ g^{-1} = g \circ h \circ g^{-1} = k \in H$, pues $g^{-1} \in \mathcal{G}$; entonces, $g^{-1} \circ k \circ g = h$ como se pide. Hemos demostrado el

Teorema XX. Si H es un subgrupo de un grupo $\mathscr{G}$ y si $g^{-1} \circ h \circ g \in H$ para todo $g \in \mathscr{G}$ y todo $h \in H$, entonces H es un subgrupo invariante de $\mathscr{G}$.

Ejemplo 10:

(*a*) Todo subgrupo H de un grupo abeliano $\mathscr{G}$ es un subgrupo invariante de $\mathscr{G}$ puesto que $g \circ h = h \circ g$ para todo $g \in \mathscr{G}$ y todo $h \in H$.

(*b*) Todo grupo $\mathscr{G}$ tiene, por lo menos, dos subgrupos invariantes: $\{u\}$, porque $u \circ g = g \circ u$ para todo $g \in \mathscr{G}$; y $\mathscr{G}$ mismo ya que para cualesquiera $g, h \in \mathscr{G}$ se tiene

$$g \circ h = g \circ h \circ (g^{-1} \circ g) = (g \circ h \circ g^{-1}) \circ g = k \circ g \quad \text{y} \quad k = g \circ h \circ g^{-1} \in \mathscr{G}$$

(*c*) Si H es un subgrupo de indice 2 de $\mathscr{G}$ [véase Ejemplo 9(*b*)], las clases laterales generadas por H consisten en H y $\mathscr{G} - H$. Luego H es un subgrupo invariante de $\mathscr{G}$.

(*d*) Para $\mathscr{G} = \{a, a^2, a^3, \ldots, a^{12} = u\}$ sus subgrupos $\{u, a^2, a^4, \ldots, a^{10}\}$, $\{u, a^3, a^6, a^9\}$, $\{u, a^4, a^8\}$ y $\{u, a^6\}$ son invariantes.

(*e*) Para el grupo octal (Problema 9), $\{u, \rho^2, \sigma^2, \tau^2\}$, $\{u, \rho^2, b, e\}$ y $\{u, \rho, \rho^2, \rho^3\}$ son subgrupos invariantes de orden 4 en tanto que $\{u, \rho^2\}$ es un subgrupo invariante de orden 2. (Empléese la Tabla 9-7 para comprobarlo.)

(*f*) El grupo octal P no es un subgrupo invariante de S_4 porque para $\rho = (1234) \in P$ y $(12) \in S_4$, se tiene $(12)^{-1} \rho (12) = (1342) \notin P$.

En el Problema 15 se demuestra el

Teorema XXI. En todo homomorfismo de un grupo $\mathscr{G}$ con operación de grupo $\circ$ y elemento neutro u en un grupo $\mathscr{G}'$ de operación de grupo $\square$ y elemento neutro u', el subconjunto S de los elementos de $\mathscr{G}$ que se aplican sobre u' es un subgrupo invariante de $\mathscr{G}$.

Este subgrupo invariante de $\mathscr{G}$ así definido se llama *núcleo* del homomorfismo.

En el Ejemplo 10(*b*) se vio que todo grupo $\mathscr{G}$ tiene $\{u\}$ y $\mathscr{G}$ mismo como subgrupos invariantes. Se les llama *impropios* al paso que otros subgrupos invariantes de $\mathscr{G}$, si los hay, se llaman *propios*. Un grupo $\mathscr{G}$, que carece de subgrupos invariantes propios se llama *simple*.

GRUPOS COCIENTES

Sea H un subgrupo invariante de un grupo $\mathscr{G}$ con la operación de grupo $\circ$ y denótese por $\mathscr{G}/H$ el conjunto de clases laterales (diferentes) según H en $\mathscr{G}$, es decir,

$$\mathscr{G}/H = \{Ha, Hb, Hc, \ldots\}$$

Se define el «producto» de pares de estas clases por

$$(Ha)(Hb) = \{(h_1 \circ a) \circ (h_2 \circ b):\ h_1, h_2 \in H\} \qquad \text{para todos los } Ha, Hb \in \mathscr{G}/H$$

y en el Problema 16 se demuestra que esta operación es bien definida.

Pero $\mathscr{G}/H$ es un grupo con respecto a la operación que se acaba de definir. Para demostrar esto observamos primero que

$$\begin{aligned}(h_1 \circ a) \circ (h_2 \circ b) &= h_1 \circ (a \circ h_2) \circ b = h_1 \circ (h_3 \circ a) \circ b \\ &= (h_1 \circ h_3) \circ (a \circ b) = h_4 \circ (a \circ b), \qquad h_3, h_4 \in H\end{aligned}$$

Entonces,

$$(Ha)(Hb) = H(a \circ b) \in G/H$$

y

$$[(Ha)(Hb)](Hc) = H[(a \circ b) \circ c] = H[a \circ (b \circ c)] = (Ha)[(Hb)(Hc)]$$

Ahora, para u, el elemento neutro de $\mathscr{G}$, $(Hu)(Ha) = (Ha)(Hu) = Ha$, de modo que $Hu = H$ es el elemento neutro de $\mathscr{G}/H$. Por último, como $(Ha)(Ha^{-1}) = (Ha^{-1})(Ha) = Hu = H$, se sigue que $\mathscr{G}/H$ contiene la inversa Ha^{-1} de toda $Ha \in \mathscr{G}/H$.

El grupo $\mathscr{G}/H$ se llama *grupo cociente* (*grupo factor*) de $\mathscr{G}$ por H.

Ejemplo 11: (*a*) Si $\mathscr{G}$ es el grupo octal del Problema 9 y $H = \{u, \rho^2, b, e\}$, es $\mathscr{G}/H = \{H, H\rho\}$. Esta representación de $\mathscr{G}/H$ no es única, desde luego. El lector demostrará que $\mathscr{G}/H = \{H, H\rho^3\} = \{H, H\sigma^2\} = \{H, H\tau^2\} = \{H, H\rho\}$.

(*b*) Para los mismos $\mathscr{G}$ y $H = \{u, \rho^2\}$, se tiene

$$\mathscr{G}/H = \{H, H\rho, H\sigma^2, Hb\} = \{H, H\rho^3, H\tau^2, He\}$$

El anterior ejemplo ilustra el

Teorema XXII. Si H de orden m, es un subgrupo invariante de $\mathscr{G}$, de orden n, el grupo cociente $\mathscr{G}/H$ es de orden n/m.

De $(Ha)(Hb) = H(a \circ b) \in \mathscr{G}/H$ obtenido antes, se sigue

Teorema XXIII. Si H es un subgrupo invariante de un grupo $\mathscr{G}$, la aplicación

$$\mathscr{G} \to \mathscr{G}/H\colon\ g \to Hg$$

es un homomorfismo de $\mathscr{G}$ sobre $\mathscr{G}/H$.

En el Problema 17 se demuestra el

Teorema XXIV. Todo grupo cociente de un grupo cíclico es cíclico.

Dejamos como ejercicio la demostración del

Teorema XXV. Si H es un subgrupo invariante de un grupo $\mathscr{G}$ y si H es también un subgrupo de un subgrupo K de $\mathscr{G}$, entonces H es un subgrupo invariante de K.

PRODUCTO DE SUBGRUPOS

Sean $H = \{h_1, h_2, \ldots, h_r\}$ y $K = \{b_1, b_2, \ldots, b_p\}$ subgrupos de un grupo $\mathscr{G}$ y defínase el «producto»

$$HK = \{h_i \circ b_j\colon\ h_i \in H,\ b_j \in K\}$$

En los Problemas 65-67 se pide al lector estudiar tales productos y, en particular, demostrar el

Teorema XXVI. Si H y K son subgrupos invariantes de un grupo $\mathscr{G}$, también lo es HK.

SERIE DE COMPOSICION

Un subgrupo invariante H de un grupo $\mathscr{G}$ se llama *maximal* si no existe ningún subgrupo invariante propio K de $\mathscr{G}$ del cual H sea un subgrupo propio.

Ejemplo 12: (*a*) A_4 del Ejemplo 4(*b*) es un subgrupo invariante maximal de S_4 porque es un subgrupo de índice 2 en S_4. Asimismo, $\{u, \rho^2, a^2, \tau^2\}$ es un subgrupo invariante maximal de A_4. (Demuéstrese.)

(*b*) El grupo cíclico $\mathscr{G} = \{u, a, a^2, \ldots, a^{11}\}$ tiene los $H = \{u, a^2, a^4, \ldots, a^{10}\}$ y $K = \{u, a^3, a^6, a^9\}$ como subgrupos invariantes maximales. Asimismo, $J = \{u, a^4, a^8\}$ es un subgrupo invariante maximal de H en tanto que $L = \{u, a^6\}$ es subgrupo invariante maximal tanto de H como de K.

Para cualquier grupo $\mathscr{G}$ una sucesión de sus subgrupos

$$\mathscr{G}, H, J, K, \ldots, U = \{u\}$$

se llama *serie de composición de* $\mathscr{G}$ si cada elemento, excepto el primero, es subgrupo invariante maximal de su precedente. Los grupos $\mathscr{G}/H$, H/J, J/K, ..., se dicen entonces los *grupos cocientes de la serie de composición*.

En el Problema 18 se demuestra

Teorema XXVII. Todo grupo finito tiene al menos una serie de composición.

Ejemplo 13: (*a*) El grupo cíclico $\mathcal{G} = \{u, a, a^2, a^3, a^4\}$ tiene solamente una serie de composición: $\mathcal{G}, U = \{u\}$.

(*b*) Una serie de composición de $\mathcal{G} = S_4$ es

$$S_4, A_4, \{(1), \rho^2, \sigma^2, \tau^2\}, \{(1), \rho^2\}, U = \{(1)\}$$

¿Es cada elemento de la serie de composición un subgrupo invariante de $\mathcal{G}$?

(*c*) Para el grupo cíclico del Ejemplo 12(*b*), hay tres series de composición: (i) $\mathcal{G}, H, J, U$, (ii) $\mathcal{G}, K, L, U$, (iii) $\mathcal{G}, H, L, U$. ¿Es todo elemento de cada serie de composición un subgrupo de $\mathcal{G}$?

En el Problema 19 se ilustra el

Teorema XXVIII (teorema de Jordan-Hölder). En todo grupo finito con distintas series de composición, todas las series son de la misma longitud, es decir, tienen igual número de elementos. Además, los grupos cocientes para cualesquiera dos series de composición se pueden aplicar biyectivamente entre sí, de modo que los grupos cocientes correspondientes son isomorfos.

Antes de intentar una demostración del Teorema XXVIII (véase Problema 23) será preciso examinar ciertas relaciones que existen entre los subgrupos de un grupo $\mathcal{G}$ y los subgrupos de sus grupos cocientes. Sea, pues, H de orden r un subgrupo invariante de un grupo $\mathcal{G}$ de orden n y escríbase:

$$S = \mathcal{G}/H = \{Ha_1, Ha_2, Ha_3, \ldots, Ha_s\}, \quad a_1 \in \mathcal{G} \tag{1}$$

donde, por comodidad, se ha hecho $a_1 = u$. Sea, además,

$$P = \{Hb_1, Hb_2, Hb_3, \cdots, Hb_p\} \tag{2}$$

un subconjunto cualquiera de S y designese por

$$K = Hb_1 \cup Hb_2 \cup Hb_3 \cup \cdots \cup Hb_p \tag{3}$$

el subconjunto de $\mathcal{G}$ cuyos elementos son los pr elementos distintos (de $\mathcal{G}$) que pertenecen a las clases de P.

Supóngase ahora que P es un subgrupo de índice t de S. Entonces $n = prt$ y alguno de los b, digamos b_1, es el elemento neutro u de $\mathcal{G}$. Se sigue que K es un subgrupo de índice t de $\mathcal{G}$ y que $P = K/H$ porque

(i) P es cerrado con respecto a la multiplicación de clases; luego K es cerrado con respecto a la operación de grupo sobre $\mathcal{G}$.
(ii) La ley asociativa rige para $\mathcal{G}$ y, por tanto, para K.
(iii) $H \in P$, luego $u \in K$.
(iv) P contiene la inversa Hb_i^{-1} de cada clase $Hb_i \in P$; luego K contiene la inversa de cada uno de sus elementos.
(v) K es de orden pr; luego K es de índice t en $\mathcal{G}$.

Recíprocamente, supóngase que K es un subgrupo de índice t de $\mathcal{G}$ que contiene a H, un subgrupo invariante de $\mathcal{G}$. Entonces, por el Teorema XXV, H es un subgrupo invariante de K y así $P = K/H$ es de índice t en $S = \mathcal{G}/H$.

Se ha demostrado el

Teorema XXIX. Sea H un subgrupo invariante de un grupo finito $\mathcal{G}$. Un conjunto P de las clases laterales de $S = \mathcal{G}/H$ es un subgrupo de índice t de S si, y solamente si, K, el conjunto de elementos del grupo que pertenecen a las clases laterales de P, es un subgrupo de índice t de $\mathcal{G}$.

Suponiendo ahora que $b_1 = u$ en (*2*) y (*3*) arriba, se establece el

Teorema XXX. Sean $\mathcal{G}$ un grupo de orden $n = rpt$, K un subgrupo de orden rp de $\mathcal{G}$ y H un subgrupo invariante de orden r de ambos K y $\mathcal{G}$. Entonces K es un subgrupo invariante de $\mathcal{G}$ si, y solamente si, $P = K/H$ es un subgrupo invariante de $S = \mathcal{G}/H$.

Para demostración, véase Problema 20.

Teorema XXXI. Sean H y K subgrupos invariantes de $\mathscr{G}$, siendo H subgrupo invariante de K, y sean $P = K/H$ y $S = \mathscr{G}/H$. Entonces, los grupos cocientes S/P y $\mathscr{G}/K$ son isomorfos.

Para demostración, véase Problema 21.

Teorema XXXII. Si H es un subgrupo invariante maximal de un grupo $\mathscr{G}$, $\mathscr{G}/H$ es simple y recíprocamente.

Teorema XXXIII Sean H y K subgrupos invariantes maximales diferentes de un grupo $\mathscr{G}$. Entonces,

(*a*) $D = H \cap K$ es un subgrupo invariante de $\mathscr{G}$, y

(*b*) H/D es isomorfo a $\mathscr{G}/K$, y K/D es isomorfo a $\mathscr{G}/H$.

Para demostración, véase Problema 22.

Problemas resueltos

1. El conjunto de clases residuales $Z/(3)$, módulo 3, ¿forma grupo con respecto a la adición?, ¿con respecto a la multiplicación?

De las tablas de adición y multiplicación para $Z/(3)$, en las que [0], [1], [2] se han remplazado por 0, 1, 2,

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabla 9-5

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Tabla 9-6

se deduce claramente que $Z/(3)$ constituye un grupo con respecto a la adición. El elemento neutro es 0 y los simétricos de 0, 1, 2 son, respectivamente, 0, 2, 1. También se ve que si bien estas clases residuales no forman grupo con respecto a la multiplicación, si se excluye la clase 0, sí lo forman. Aquí el elemento neutro es 1 y cada uno de los elementos 1, 2 es su propio simétrico.

2. ¿Forman grupo respecto a la multiplicación las clases residuales módulo 4, excluyendo la clase 0?

De la Tabla 5·2 del Ejemplo 12, Capítulo 5, página 53, se saca que estas clases residuales no forman grupo con respecto a la multiplicación.

3. Demostrar: Si $a, b, c \in \mathscr{G}$, $a \circ b = a \circ c$ (también $b \circ a = c \circ a$) implica $b = c$.

Sea $a \circ b = a \circ c$. Operando a la izquierda por $a^{-1} \in \mathscr{G}$, se tiene $a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$. Por la ley asociativa, $(a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$; luego $u \circ b = u \circ c$ y resulta $b = c$. Del mismo modo, $(b \circ a) \circ a^{-1} = (c \circ a) \circ a^{-1}$ se reduce a $b = c$.

4. Demostrar: Si $a, b \in \mathscr{G}$, las ecuaciones $a \circ x = b$ y $y \circ a = b$ tienen solución única.

Se obtiene fácilmente $x = a^{-1} \circ b$ y $y = b \circ a^{-1}$ como soluciones. Para probar la unicidad, supongamos que x' y y' sean otras soluciones. Entonces $a \circ x = a \circ x'$ y asimismo $y \circ a = y' \circ a$, de donde, por el Teorema 1, $x = x'$ y $y = y'$.

5. Demostrar: Para todo $a \in \mathscr{G}$, $a^m \circ a^n = a^{m+n}$ con $m, n \in Z$.

Consideremos los casos según que m y n sean positivos, de distinto signo o uno de ellos nulo. Si m y n son positivos,

$$a^m \circ a^n = (\overbrace{a \circ a \circ \cdots \circ a}^{m \text{ factores}}) \circ (\overbrace{a \circ a \circ \cdots \circ a}^{n \text{ factores}}) = \overbrace{a \circ a \circ \cdots \circ a}^{m+n \text{ factores}} = a^{m+n}$$

Si $m = -r$ y $n = s$, de donde r y s son enteros positivos,

$$a^m \circ a^n = a^{-r} \circ a^s = (a^{-1})^r \circ a^s = (a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}) \circ (a \circ a \circ \cdots \circ a)$$

$$= \begin{cases} a^{s-r} = a^{m+n} & \text{si } s \geq r \\ (a^{-1})^{r-s} = a^{s-r} = a^{m+n} & \text{si } s < r \end{cases}$$

Los otros casos se dejan al lector.

6. Demostrar: Un subconjunto no vacío $\mathscr{G}'$ de un grupo $\mathscr{G}$ es un subgrupo de $\mathscr{G}$ si, y solamente si, para cualesquiera $a, b \in \mathscr{G}'$, $a^{-1} \circ b \in \mathscr{G}'$.

Supóngase que $\mathscr{G}'$ es un subgrupo de $\mathscr{G}$. Si $a, b \in \mathscr{G}'$, entonces $a^{-1} \in \mathscr{G}'$ y, por la ley de clausura, también lo es $a^{-1} \circ b$.

Recíprocamente, supóngase que $\mathscr{G}'$ es un subconjunto no vacío de $\mathscr{G}$ para el cual $a^{-1} \circ b \in \mathscr{G}'$ siempre que $a, b \in \mathscr{G}'$. Como entonces $a^{-1} \circ a = u \in \mathscr{G}'$, es $u \circ a^{-1} = a^{-1} \in \mathscr{G}'$ y todo elemento de $\mathscr{G}'$ tiene un inverso en $\mathscr{G}'$. Por último, para cualesquiera $a, b \in \mathscr{G}'$, $(a^{-1})^{-1} \circ b = a \circ b \in \mathscr{G}'$, y se cumple la ley de clausura. Así que $\mathscr{G}'$ es un grupo y, por tanto, un subgrupo de $\mathscr{G}$.

7. Demostrar: Si S es un conjunto de subgrupos de un grupo $\mathscr{G}$, la intersección de estos subgrupos es también un subgrupo de $\mathscr{G}$.

Sean a y b elementos de la intersección y, por tanto, elementos de cada uno de los subgrupos que forman S. Por el Teorema VIII, $a^{-1} \circ b$ pertenece a cada subgrupo y, por consiguiente, a la intersección. Así, pues, la intersección es un subgrupo de $\mathscr{G}$.

8. Demostrar: Todo subgrupo de un grupo cíclico es un grupo cíclico.

Sea $\mathscr{G}'$ un subgrupo de un grupo cíclico $\mathscr{G}$ de generador a. Supóngase que m es el mínimo entero positivo para el cual $a^m \in \mathscr{G}'$. Siendo entonces todo elemento de $\mathscr{G}'$ un elemento de $\mathscr{G}$, es de la forma a^k, $k \in Z$. Escribiendo

$$k = mq + r, \qquad 0 \leq r < m$$

tenemos

$$a^k = a^{mq+r} = (a^m)^q \circ a^r$$

y, por tanto,

$$a^r = (a^m)^{-q} \circ a^k$$

Como ambos a^m y $a^k \in \mathscr{G}'$ se sigue que $a^r \in \mathscr{G}'$. Pero como $r < m$, $r = 0$. Así, pues, $k = mq$, todo elemento de $\mathscr{G}'$ es de la forma $(a^m)^q$ y $\mathscr{G}$ es el grupo cíclico generado por a^m.

9. El subconjunto $\{u = (1), \rho, \rho^2, \rho^3, \sigma^2, \tau^1, b = (13), e = (24)\}$ de S_4 es un grupo (véase la Tabla 9-7) que se llama *grupo octal de un cuadrado* o *grupo diédrico*. Vamos a demostrar que este grupo de permutaciones se puede obtener por propiedades de simetría de un cuadrado.

Considérese el cuadrado (Fig. 9-1) con los vértices numerados 1, 2, 3, 4; trácense las diagonales 1O3 y 2O4, las paralelas medias AOB y COD. Vamos a examinar todos los movimientos rígidos (rotaciones en el plano en torno a O y en el espacio en torno a las diagonales y las paralelas medias) tales que el cuadrado parezca el mismo que antes después del movimiento.

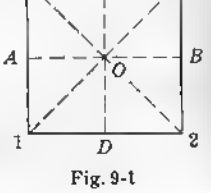


Fig. 9-1

Denótese por ρ la rotación en sentido contrario a las agujas del reloj del cuadrado en torno a O de 90°. Su efecto es llevar 1 a 2, 2 a 3, 3 a 4 y 4 a 1; así, pues, $\rho = (1234)$. Ahora bien, $\rho^2 = \rho \circ \rho = (13)(24)$ es una rotación de 180° en torno

a O, $\rho^3 = (1432)$ es una rotación de 270° y $\rho^4 = (1) = u$ es una rotación en torno a O de 360° o de 0°. Las rotaciones de 180° en torno a los ejes medios AOB y COD dan lugar, respectivamente, a $\sigma^2 = (14)(23)$ y a $\tau^2 = (12)(34)$ mientras que las rotaciones de 180° en torno a las diagonales $1O3$ y $2O4$ dan lugar a $c = (24)$ y a $b = (13)$.

La tabla de operación para este grupo es

	u	ρ	ρ^2	ρ^3	σ^2	τ^2	b	c
u	u	ρ	ρ^2	ρ^3	σ^2	τ^2	b	c
ρ	ρ	ρ^2	ρ^3	u	b	c	τ^2	σ^2
ρ^2	ρ^2	ρ^3	u	ρ	τ^2	σ^2	c	b
ρ^3	ρ^3	u	ρ	ρ^2	c	b	σ^2	τ^2
σ^2	σ^2	c	τ^2	b	u	ρ^2	ρ^3	ρ
τ^2	τ^2	b	σ^2	c	ρ^2	u	ρ	ρ^3
b	b	σ^2	c	τ^2	ρ	ρ^3	u	ρ^2
c	c	τ^2	b	σ^2	ρ^3	ρ	ρ^2	u

Tabla 9-7

Para formar la tabla

(1) llenar la primera fila y la primera columna y complétese la parte superior izquierda de 4 × 4 casillas.

(2) complétese la segunda fila, $\left(\rho \circ \sigma^2 = (1234) \circ (14)(23) = (13) = b, \ \ldots\right)$

y luego la tercera y cuarta filas,

$$\left(\rho^2 \circ \sigma^2 = \rho \circ (\rho \circ \sigma^2) = \rho \circ b = \tau^2, \ \ldots\right)$$

(3) complétese la segunda columna y luego la tercera y cuarta columnas,

$$\left(\sigma^2 \circ \rho^2 = (\sigma^2 \circ \rho) \circ \rho = c \circ \rho = \tau^2, \ \ldots\right)$$

(4) termínese la tabla, $\left(\sigma^2 \circ \tau^2 = \sigma^2 \circ (\sigma^2 \circ \rho^2) = \rho^2, \ \ldots\right)$

10. Un grupo de permutación de n símbolos se dice *regular* si cada uno de sus elementos excepto el neutro mueve todos los n símbolos. Hallar los grupos de permutación regulares de 4 símbolos.

Utilizando el Ejemplo 4, los grupos que se piden son:

$$\{\rho, \rho^2, \rho^3, \rho^4 = (1)\}, \quad \{\sigma, \sigma^2, \sigma^3, \sigma^4 = (1)\}, \quad \text{y} \quad \{\tau, \tau^2, \tau^3, \tau^4 = (1)\}$$

11. Demostrar: La aplicación $Z \to Z/(n)$: $m \to [m]$ es un homomorfismo del grupo aditivo Z sobre el grupo aditivo $Z/(n)$ de los enteros módulo n.

Como $[m] = [r]$ siempre que $m = nq + r$, $0 \leq r < n$, es evidente que la aplicación no es inyectiva. No obstante, todo $m \in Z$ tiene una imagen única en el conjunto $\{[0], [1], [2], \ldots, [n-1]\}$ de las clases residuales módulo n, y todo elemento de este último conjunto es imagen. Asimismo, si $a \to [r]$ y $b \to [s]$, entonces $a + b \to [r] + [s] = [t]$ la clase residual módulo n de $c = a + b$. De modo que las operaciones de grupo se preservan y la aplicación es un homomorfismo de Z sobre $Z/(n)$.

12. Demostrar que en un isomorfismo entre dos grupos $\mathscr{G}$ y $\mathscr{G}'$ los elementos neutros se corresponden y si $x \in \mathscr{G}$ y $x' \in \mathscr{G}'$ se corresponden, lo mismo ocurre con sus inversos.

Denótese el elemento neutro de $\mathscr{G}$ por u y el de $\mathscr{G}'$ por u'. Supóngase ahora que $u \to v'$ y que para $x \neq u$, $x \to x'$. Entonces $x = u \circ x \to v' \square x' = x' = u' \square x'$, de donde, por la ley de cancelación, $v' = u'$ y tenemos la primera parte del teorema.

Para la segunda parte, supóngase $x \to x'$ y $x^{-1} \to y'$. Entonces, $u = x \circ x^{-1} \to x' \square y' = u' = x' \square (x')^{-1}$ de modo que $y' = (x')^{-1}$.

13. Demostrar: Todo grupo cíclico de orden infinito es isomorfo al grupo aditivo Z.

Considérese el grupo cíclico infinito $\mathscr{G}$ generado por a y sea la aplicación

$$n \to a^n, \quad n \in Z$$

de Z en $\mathscr{G}$. Esta aplicación es evidentemente sobreyectiva y, además, inyectiva, pues si para $s > t$ se tuviera $s \leftrightarrow a^s$ y $t \leftrightarrow a^t$ con $a^s = a^t$, entonces $a^{s-t} = u$ y $\mathscr{G}$ sería finito. Por último, $s + t \leftrightarrow a^{s+t} = a^s \cdot a^t$ y la aplicación es un isomorfismo.

14. Demostrar: Todo grupo finito de orden n es isomorfo a un grupo de permutación de n símbolos.

Sea $\mathscr{G} = \{g_1, g_2, g_3, \ldots, g_n\}$ con la operación de grupo $\sqcap$ y defínase

$$p_j = \begin{pmatrix} g_i \\ g_i \sqcap g_j \end{pmatrix} = \begin{pmatrix} g_1 & g_2 & g_3 & \cdots & g_n \\ g_1 \sqcap g_j & g_2 \sqcap g_j & g_3 \sqcap g_j & \cdots & g_n \sqcap g_j \end{pmatrix}, \qquad (j = 1, 2, 3, \ldots, n)$$

Los elementos de la segunda fila de p_j son los de la columna encabezada por g_j en la tabla de operación de $\mathscr{G}$ y, por tanto, constituyen una permutación de los elementos que encabezan las filas. Así, pues, $P = \{p_1, p_2, p_3, \ldots, p_n\}$ es un subconjunto de los elementos del grupo simétrico S_n de n símbolos. Se deja al lector demostrar que P cumple las condiciones del Teorema VII para ser un grupo. Considérese ahora la biyección

$$(a) \qquad g_i \leftrightarrow p_i, \quad i = 1, 2, 3, \ldots, n$$

Si $g_t = g_r \sqcap g_s$, luego $g_i \leftrightarrow p_r \circ p_s$ de modo que

$$g_t \leftrightarrow \begin{pmatrix} g_i \\ g_i \sqcap g_r \end{pmatrix} \circ \begin{pmatrix} g_i \\ g_i \sqcap g_s \end{pmatrix} = \begin{pmatrix} g_i \\ g_i \sqcap g_r \end{pmatrix} \circ \begin{pmatrix} g_i \sqcap g_r \\ g_i \sqcap g_r \sqcap g_s \end{pmatrix} = \begin{pmatrix} g_i \\ g_i \sqcap g_t \end{pmatrix}$$

y (a) es un isomorfismo de $\mathscr{G}$ sobre P. Nótese que P es regular.

15. Demostrar: En cualquier homomorfismo de un grupo $\mathscr{G}$ con operación de grupo $\circ$ y elemento neutro u en un grupo $\mathscr{G}'$ de operación de grupo $\sqcap$ y elemento neutro u', el subconjunto S de los elementos de $\mathscr{G}$ que se aplican sobre u', es un subgrupo invariante de $\mathscr{G}$.

Como consecuencias del Teorema XIII, se tienen

(a) $u \to u'$; luego, S no es vacío.

(b) Si $a \in S$, es $a^{-1} \to (u')^{-1} = u'$; luego, $a^{-1} \in S$.

(c) Si $a, b \in S$, es $a^{-1} \circ b \to u' \sqcap u' = u'$; luego, $a^{-1} \circ b \in S$.

Así que S es un subgrupo de $\mathscr{G}$.

Para cualesquiera $a \in S$ y $g \in \mathscr{G}$,

$$g^{-1} \circ a \circ g \to (g')^{-1} \sqcap u' \sqcap g' = u'$$

de tal modo que $g^{-1} \circ a \circ g \in S$. Y por el Teorema XX, S es un subgrupo invariante de $\mathscr{G}$, como se afirmaba.

16. Demostrar: El producto de clases laterales

$$(Ha)(Hb) = \{(h_1 \circ a) \circ (h_2 \circ b) : h_1, h_2 \in H\} \qquad \text{para todo } Ha, Hb \in \mathscr{G}/H$$

donde H es un subgrupo invariante de $\mathscr{G}$, es bien definido.

Ante todo, demostramos: Para cualesquiera $x, x' \in \mathscr{G}$, es $Hx' = Hx$ si, y solamente si, $x' = v \circ x$ para algún $v \in H$. Supóngase que $Hx' = Hx$. Entonces $x' \in Hx$ requiere que $x' = v \circ x$ para algún $v \in H$. Recíprocamente, si $x' = v \circ x$ con $v \in H$, entonces $Hx' = H(v \circ x) = (Hv)x = Hx$.

Sean ahora Ha' y Hb' otras representaciones de Ha y Hb, respectivamente, con $a' = a \circ r$, $b' = b \circ s$ y $r, s \in H$. En $(Ha')(Hb') = \{[h_1 \circ (a \circ r)] \circ [h_2 \circ (b \circ s)] : h_1, h_2 \in H\}$ se tiene, mediante (i'_2), página 87,

$$\begin{aligned} [h_1 \circ (a \circ r)] \circ [h_2 \circ (b \circ s)] &= (h_1 \circ a) \circ (r \circ h_2) \circ (b \circ s) \\ &= (h_1 \circ a) \circ h_3 \circ (t \circ b) = (h_1 \circ a) \circ (h_3 \circ t) \circ b \\ &= (h_1 \circ a) \circ (h_4 \circ b) \qquad \text{pero} \quad h_3, t, h_4 \in H \end{aligned}$$

Entonces, $$(Ha')(Hb') = (Ha)(Hb)$$

y el producto $(Ha)(Hb)$ está bien definido

17. Demostrar: Todo grupo cociente de un grupo cíclico $\mathscr{G}$ es cíclico.

Sea H un subgrupo cualquiera (invariante) del grupo cíclico $\mathscr{G} = \{u, a, a^2, \ldots, a^r\}$ y considérese el homomorfismo

$$\mathscr{G} \to \mathscr{G}/H : a^i \to Ha^i$$

Puesto que todo elemento de $\mathscr{G}/H$ es de la forma Ha^i para algún $a^i \in \mathscr{G}$ y $Ha^i = (Ha)^i$ (demuéstrese), se sigue que todo elemento de $\mathscr{G}/H$ es potencia de $b = Ha$. Luego G/H es cíclico.

18. Demostrar: Todo grupo finito $\mathscr{G}$ tiene al menos una serie de composición.

(i) Supóngase que $\mathscr{G}$ es simple: entonces $\mathscr{G}, U$ es una serie de composición.

(ii) Supóngase que $\mathscr{G}$ no es simple; entonces existe un subgrupo invariante $H \neq \mathscr{G}, U$ de $\mathscr{G}$. Si H es maximal en $\mathscr{G}$ y U es maximal en H, entonces $\mathscr{G}, H, U$ es una serie de composición. Supóngase que H no es maximal en $\mathscr{G}$ pero que U sí es maximal en H; hay entonces un subgrupo invariante K de $\mathscr{G}$ tal que H es subgrupo invariante de K. Si K es maximal en $\mathscr{G}$ y H es maximal en K, entonces $\mathscr{G}, K, H, U$ es una serie de composición. Supóngase ahora que H es maximal en $\mathscr{G}$, pero que U no es maximal en H; existe entonces un subgrupo invariante J de H. Si J es maximal en H y U es maximal en J, entonces $\mathscr{G}, H, J, U$ es una serie de composición. Supóngase ahora que H no es maximal en $\mathscr{G}$ y que U no es maximal en H; entonces . . . Como $\mathscr{G}$ es finito, hay solamente un número finito de subgrupos y, por último, debe llegarse a una serie de composición.

19. Considérense dos series de composición del grupo cíclico de orden 60: $G = \{u, a, a^2, \ldots, a^{59}\}$:

$$G, H = \{u, a^2, a^4, \ldots, a^{58}\}, \quad J = \{u, a^4, a^8, \ldots, a^{56}\}, \quad K = \{u, a^{12}, a^{24}, a^{36}, a^{48}\}, \quad U = \{u\}$$

y

$$G, M = \{u, a^3, a^6, \ldots, a^{57}\}, \quad N = \{u, a^{15}, a^{30}, a^{45}\}, \quad P = \{u, a^{30}\}, \quad U$$

Los grupos cocientes son:

$$G/H = \{H, Ha\}, \quad H/J = \{J, Ja^2\}, \quad J/K = \{K, Ka^4, Ka^8\}, \quad K/U = \{U, Ua^{12}, Ua^{24}, Ua^{36}, Ua^{48}\}$$

y

$$G/M = \{M, Ma, Ma^2\}, \quad M/N = \{N, Na^3, Na^6, Na^9, Na^{12}\}, \quad N/P = \{P, Pa^{15}\}, \quad P/U = \{U, Ua^{30}\}$$

Entonces en la biyección $\mathscr{G}/H \leftrightarrow N/P$, $H/J \leftrightarrow P/U$, $J/K \leftrightarrow \mathscr{G}/M$, $K/U \leftrightarrow M/N$, los grupos cocientes correspondientes son isomorfos por las aplicaciones

$H \leftrightarrow P$	$J \leftrightarrow U$	$K \leftrightarrow M$	$U \leftrightarrow N$
$Ha \leftrightarrow Pa^{15}$	$Ja^2 \leftrightarrow Ua^{30}$	$Ka^4 \leftrightarrow Ma$	$Ua^{12} \leftrightarrow Na^3$
		$Ka^8 \leftrightarrow Ma^2$	$Ua^{24} \leftrightarrow Na^6$
			$Ua^{36} \leftrightarrow Na^9$
			$Ua^{48} \leftrightarrow Na^{12}$

20. Demostrar: Sean $\mathscr{G}$ un grupo de orden $n = rpt$, K un subgrupo de $\mathscr{G}$ de orden rp y H un subgrupo invariante de orden r tanto de K como de $\mathscr{G}$. Entonces, K es un subgrupo invariante de $\mathscr{G}$ si, y solo si, $P = K/H$ es subgrupo invariante de $S = \mathscr{G}/H$.

Sean g un elemento cualquiera de $\mathscr{G}$ y $K = \{b_1, b_2, \ldots, b_{rp}\}$.

Supóngase que P es un subgrupo invariante de S. Para $Hg \in S$, se tiene

(i) $$(Hg)P = P(Hg)$$

Así, pues, para todo $Hb_i \in P$ existe $Hb_j \in P$ tal que

(ii) $$(Hg)(Hb_i) = (Hb_j)(Hg)$$

Además, $(Hg)(Hb_i) = (Hb_j)(Hg) = (Hg)(Hb_k)$ implica $Hb_i = Hb_k$. Entonces,

(iii) $$Hb_i = (Hg^{-1})(Hb_j)(Hg) = g^{-1}(Hb_j)g$$

(iv) $$K = Hb_1 \cup Hb_2 \cup \cdots \cup Hb_p = g^{-1}Kg$$

y

(v) $$gK = Kg$$

Así, pues, K es un subgrupo invariante de $\mathscr{G}$.

Recíprocamente, supóngase que K es un subgrupo invariante de $\mathscr{G}$. Entonces, con solo invertir los pasos anteriores, se concluye que P es un subgrupo invariante de S.

21. Demostrar: Sean H y K subgrupos invariantes de $\mathscr{G}$ con H subgrupo invariante de K y sean $P = K/H$ y $S = \mathscr{G}/H$. Entonces los grupos cocientes S/P y $\mathscr{G}/K$ son isomorfos.

Sean $n = rpt, rp, r$ los respectivos órdenes de $\mathscr{G}, K, H$. Entonces K es un subgrupo invariante de indice t en $\mathscr{G}$ y definiendo

$$\mathscr{G}/K = \{Kc_1, Kc_2, \ldots, Kc_t\}, \qquad c_i \in \mathscr{G}$$

Por el Teorema XXX, P es un subgrupo invariante de S; así que P hace una partición de S en t clases laterales de modo que se puede escribir

$$S/P = \{P(Ha_{i_1}), P(Ha_{i_2}), \ldots, P(Ha_{i_t})\}, \qquad Ha_{i_j} \in S$$

Pero los elementos de $\mathscr{G}$ que constituyen el subgrupo K por la partición en clases laterales según H, forman P. De modo que cada c_k se encuentra en una, y solo una, de las Ha_{i_j}. Por tanto, reordenando las clases de S/P si fuera necesario, podemos escribir

$$S/P = \{P(Hc_1), P(Hc_2), \ldots, P(Hc_t)\}$$

La aplicación pedida es $\mathscr{G}/K \leftrightarrow S/P : \; Kc_i \leftrightarrow P(Hc_i)$

22. Demostrar: Sean H y K subgrupos invariantes maximales distintos de un grupo $\mathscr{G}$. Entonces, (*a*) $D = H \cap K$ es un subgrupo invariante de $\mathscr{G}$ y (*b*) H/D es isomorfo a $\mathscr{G}/K$ y K/D es isomorfo a $\mathscr{G}/H$.

(*a*) Por el Teorema X, D es un subgrupo de $\mathscr{G}$. Como H y K son subgrupos invariantes de $\mathscr{G}$, tenemos para cada $d \in D$ y todo $g \in \mathscr{G}$,

$$g^{-1} \circ d \circ g \in H, \quad g^{-1} \circ d \circ g \in K \quad \text{y así} \quad g^{-1} \circ d \circ g \in D$$

Así, pues, para todo $g \in \mathscr{G}$, $g^{-1}Dg = D$ y D es un subgrupo invariante de $\mathscr{G}$.

(*b*) Por el Teorema XXV, D es un subgrupo invariante de H y de K. Suponiendo

(i) $$H = Dh_1 \cup Dh_2 \cup \ldots \cup Dh_n, \qquad h_i \in H$$

entonces, como $K(Dh_i) = (KD)h_i = Kh_i$. (¿Por qué?)

(ii) $$KH = Kh_1 \cup Kh_2 \cup \ldots \cup Kh_n$$

Por el Teorema XXVI, $HK = KH$ es un subgrupo de $\mathscr{G}$. Entonces, como H es un subgrupo propio de HK y, por hipótesis, es un subgrupo invariante maximal de $\mathscr{G}$, se sigue que $HK = \mathscr{G}$.

De (i) y (ii) se obtiene

$$H/D = \{Dh_1, Dh_2, \ldots, Dh_n\} \quad \text{y} \quad \mathscr{G}/K = \{Kh_1, Kh_2, \ldots, Kh_n\}$$

Por la aplicación biyectiva

$$Dh_i \leftrightarrow Kh_i, \qquad (i = 1, 2, 3, \ldots, n)$$

$$(Dh_i)(Dh_j) = D(h_i \circ h_j) \leftrightarrow K(h_i \circ h_j) = (Kh_i)(Kh_j)$$

y H/D es isomorfo a $\mathscr{G}/K$. Se deja al lector la demostración de que K/D y $\mathscr{G}/H$ son isomorfos.

23. Demostrar: Para un grupo finito con distintas series de composición, todas las series son de igual longitud, es decir, tienen el mismo número de elementos. Además, los grupos cocientes para cualesquiera pares de series de composición pueden ponerse en correspondencia biunívoca de modo que los grupos cocientes correspondientes sean isomorfos.

Sea (*a*) $$\mathscr{G}, H_1, H_2, H_3, \ldots, H_r = U$$

(*b*) $$\mathscr{G}, K_1, K_2, K_3, \ldots, K_s = U$$

dos series de composición distintas de $\mathscr{G}$. Ahora bien, el teorema es cierto para todo grupo de orden uno. Aceptemos que es cierto para todos los grupos de orden menor que el de $\mathscr{G}$. Consideramos dos casos:

(i) $H_1 = K_1$. Después de quitar $\mathscr{G}$ de (*a*) y (*b*) quedan dos series de composición de H_1 para las cuales, por hipótesis, el teorema se verifica. Desde luego, también seguirá verificándose cuando $\mathscr{G}$ se pone en cada una.

(ii) $H_1 \neq K_1$. Escríbase $D = H_1 \cap K_1$. Como $\mathscr{G}/H_1$ (también $\mathscr{G}/K_1$) es simple y, por el Teorema XXXIII, es isomorfo a K_1/D (también $\mathscr{G}/K_1$ es isomorfo a H_1/D) entonces K_1/D (y también H_1/D) es simple. Luego D es el subgrupo invariante maximal de ambos H_1 y K_1 y así $\mathscr{G}$ tiene las series de composición

$$(a') \qquad \mathscr{G},\ H_1,\ D,\ D_1,\ D_2,\ D_3,\ \ldots,\ D_t = U$$

y

$$(b') \qquad \mathscr{G},\ K_1,\ D,\ D_1,\ D_2,\ D_3,\ \ldots,\ D_t = U$$

Si se escriben los grupos cocientes en el orden

$$\mathscr{G}/H_1,\ H_1/D,\ D/D_1,\ D_1/D_2,\ D_2/D_3,\ \ldots,\ D_{t-1}/D_t$$

y

$$K_1/D,\ G/K_1,\ D/D_1,\ D_1/D_2,\ D_2/D_3,\ \ldots,\ D_{t-1}/D_t,$$

los grupos cocientes correspondientes son isomorfos, es decir, $\mathscr{G}/H_1$ y K_1/D, H_1/D y $\mathscr{G}/K_1$, D/D_1 y D/D_1, ..., son isomorfos.

Pero por (i) los grupos cocientes definidos por (a) y (a') [también por (b) y (b')], se pueden poner en correspondencia biunívoca o biyección, de modo que los grupos cocientes correspondientes sean isomorfos. Así, pues, los grupos cocientes definidos por (a) y (b) son isomorfos en cierto orden, como se requería.

Problemas propuestos

24. Cuáles de los siguientes conjuntos forman grupo con respecto a la operación que se indica:

(a) $S = \{x: x \in Z,\ x < 0\}$; adición

(b) $S = \{5x: x \in Z\}$; adición

(c) $S = \{x: x \in Z,\ x$ es único$\}$; multiplicación

(d) Las n raíces n-simas de 1; multiplicación

(e) $S = \{-2, -1, 1, 2\}$; multiplicación

(f) $S = \{1, -1, i, -i\}$; multiplicación

(g) El conjunto de clases residuales m; adición

(h) $S = \{[a]: [a] \in Z/(m),\ (a, m) = 1\}$; multiplicación

(i) $S = \{z: z \in C,\ |z| = 1\}$; multiplicación

Resp. (a), (c), (e), no lo son.

25. Demostrar que las clases residuales no nulas módulo p forman un grupo con respecto a la multiplicación si, y solo si, p es primo.

26. ¿Cuáles de los siguientes subconjuntos de $Z/(13)$ forman grupo con respecto a la multiplicación: (a) $\{[1], [12]\}$; (b) $\{[1], [2], [4], [6], [8], [10], [12]\}$; (c) $\{[1], [5], [8], [12]\}$? *Resp.* (a), (c).

27. Considérese el sistema de coordenadas rectangulares en el espacio. Denótese por a, b, c, respectivamente, las rotaciones en sentido de las agujas del reloj de 180° en torno a los ejes X, Y, Z y por u la posición original. Completar la tabla adjunta para que se vea que $\{u, a, b, c\}$ es un grupo, el grupo cuaternario de Klein.

$\circ$	u	a	b	c
u	u	a	b	c
a	a			
b	b	c		
c	c	b	a	

Tabla 9-8

28. Demostrar el Teorema III, página 83.

Sugerencia: $u^{-1} \circ x = u$ tiene $x = u$ y $x = (a^{-1})^{-1}$ como soluciones.

29. Demostrar el Teorema IV, página 83.

Sugerencia. Considérese $(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1}$

30. Demostrar el Teorema V, página 83.

31. Demostrar: $a^{-m} = (a^m)^{-1}$, $m \in Z$.

32. Completar la demostración del Teorema VI, página 83.

33. Demostrar los Teoremas IX y XI de la página 84 y el Teorema XIV de la página 85.

34. Demostrar: Todo subgrupo $\mathscr{G}'$ de un grupo $\mathscr{G}$ tiene el elemento neutro u de $\mathscr{G}$, como elemento neutro.

35. Enumerar todos los subgrupos propios del grupo aditivo $Z/(18)$.

36. Sean $\mathscr{G}$ un grupo con respecto a $\circ$ y a un elemento cualquiera de $\mathscr{G}$. Demostrar que

$$H = \{x: x \in \mathscr{G},\ x \circ a = a \circ x\}$$

es un subgrupo de $\mathscr{G}$.

37. Demostrar: Todo subgrupo propio de un grupo abeliano es abeliano. Establecer la recíproca y demostrar con un ejemplo que es falsa.

38. Demostrar: El orden de $a \in \mathscr{G}$ es el orden del subgrupo cíclico generado por a.

39. Averiguar el orden de los elementos (*a*) (123), (*b*) (1432), (*c*) (12)(34) de S_4.
Resp. (*a*) 3, (*b*) 4, (*c*) 2.

40. Verificar que el subconjunto A_n de todas las permutaciones pares de S_n forma un subgrupo de S_n. Demostrar que cada elemento de A_n deja invariante el polinomio del Problema 12, Capítulo 2, página 27.

41. Demostrar que el conjunto $\{x: x \in Z,\ 5 \mid x\}$ es un subgrupo del grupo aditivo Z.

42. Formar una tabla de operación para investigar si (1), (12)(34), (13)(24), (14)(23) es un grupo de permutación regular de cuatro símbolos.

43. Determinar el subconjunto de S_4 que deja (*a*) el elemento 2 invariante, (*b*) los elementos 2 y 4 invariantes, (*c*) $x_1x_2 + x_3x_4$ invariante, (*d*) $x_1x_2 + x_3 + x_4$ invariante.

Resp. (*a*) {(1), (13), (14), (34), (134), (143)} (*c*) {(1), (12), (34), (12)(34), (13)(24), (14)(23), (1423), (1324)}
(*b*) {(1), (13)} (*d*) {(1), (12), (34), (12)(34)}

44. Demostrar la segunda parte del Teorema XV, página 86. *Sugerencia*: emplear $[m] \leftrightarrow a^m$.

45. Demostrar que el grupo cuaternario de Klein es isomorfo al subgrupo $P = \{(1), (12)(34), (13)(24), (14)(23)\}$ de S_4.

46. Demostrar que el grupo del Ejemplo 7 es isomorfo al grupo de permutación

$$P = \{(1), (12)(35)(46), (14)(25)(36), (13)(26)(45), (156)(243), (165)(234)\}$$

de seis símbolos.

47. Demostrar que los elementos no nulos de $Z/(13)$, con respecto a la multiplicación, forman un grupo cíclico isomorfo al grupo aditivo $Z/(12)$. Hallar todos los isomorfismos entre los dos grupos.

48. Demostrar: Los únicos grupos de orden 4 son el grupo cíclico de orden 4 y el grupo cuaternario de Klein.
Sugerencia: $\mathscr{G} = \{u, a, b, c\}$ o bien tiene un elemento de orden 4 o todos sus elementos excepto u tienen orden 2. En el último caso, $a \circ b \neq a, b, u$ por las leyes de cancelación.

49. Sea S un subgrupo de un grupo $\mathscr{G}$ y defínase $T = \{x: x \in \mathscr{G},\ Sx = xS\}$. Demostrar que T es un subgrupo de $\mathscr{G}$.

50. Demostrar: Dos clases a la derecha Ha y Hb según un subgrupo H de un grupo $\mathscr{G}$ son idénticas si, y solo si, $ab^{-1} \in H$.

51. Demostrar: $a \in Hb$ implica $Ha = Hb$ donde H es un subgrupo de $\mathscr{G}$ y $a, b \in \mathscr{G}$.

52. Enumerar todas las clases del subgrupo $\{(1), (12)(34)\}$ en el grupo octal.

53. Formar la tabla de operación para el grupo simétrico S_3 de tres símbolos. Enumerar sus subgrupos propios y obtener las clases a la derecha y a la izquierda para cada uno. ¿Es S_3 simple?

54. Obtener el grupo simétrico del Problema 53 utilizando las propiedades de simetría de un triángulo equilátero.

55. Obtener el subgrupo $\{u, \rho^2, \sigma^2, \tau^2\}$ de S_4 utilizando las propiedades de simetría de un rectángulo (no cuadrado).

56. Obtener el grupo alternante A_4 de S_4 utilizando las propiedades de simetría del tetraedro regular.

57. Demostrar el Teorema XXV, página 89.

58. Demostrar que $K = \{u, \rho^2, \sigma^2, \tau^2\}$ es un subgrupo invariante de S_4. Obtener S_4/K y escribir completo el homomorfismo $S_4 \to S_4/K$: $x \to Kx$.
Respuesta parcial. $U \to K$, $(12) \to K(12)$, $(13) \to K(13)$, ... $(24) \to K(13)$, $(34) \to K(12)$, ...

59. Utilizar $K = \{u, \rho^2, \sigma^2, \tau^2\}$, subgrupo invariante de S_4 y $H = \{u, \sigma^2\}$, subgrupo invariante de K, para demostrar que un subgrupo invariante propio de un subgrupo invariante propio de un grupo $\mathcal{G}$ no es necesariamente un subgrupo invariante de $\mathcal{G}$.

60. Demostrar: El grupo aditivo $Z/(m)$ es un grupo cociente del grupo aditivo Z.

61. Demostrar: Si H es un subgrupo invariante de un grupo $\mathcal{G}$, el grupo cociente $\mathcal{G}/H$ es cíclico si el índice de H en $\mathcal{G}$ es primo.

62. Demostrar que la aplicación $\begin{cases} (1), \rho^2, \sigma^2, \tau^2 \to u \\ \alpha, \beta^2, \gamma, \delta^3 \to a \\ \alpha^2, \beta, \gamma^3, \delta \to a^2 \end{cases}$ define un homomorfismo de A_4 sobre $\mathcal{G} = \{u, a, a^2\}$. Nótese que el subconjunto de A_4 que se aplica sobre el elemento neutro de $\mathcal{G}$ es un subgrupo invariante de A_4.

63. Demostrar: En un homomorfismo de un grupo $\mathcal{G}$ sobre un grupo $\mathcal{G}'$, sea H el conjunto de todos los elementos de $\mathcal{G}$ que se aplican en $u' \in \mathcal{G}'$. Entonces el grupo cociente de $\mathcal{G}/H$ es isomorfo a $\mathcal{G}'$.

64. Establecer un homomorfismo del grupo octal sobre $\{u, a\}$.

65. Si $H = \{u, \alpha, \alpha^2\}$ y $K = \{u, \beta, \beta^2\}$ son subgrupos de S_4, demostrar que $HK \neq KH$. Utilizar HK y KH para verificar que, en general, el producto de dos subgrupos de un grupo $\mathcal{G}$ no es un subgrupo de $\mathcal{G}$.

66. Demostrar: Si $H = \{h_1, h_2, \ldots, h_r\}$ y $K = \{b_1, b_2, \ldots, b_s\}$ son subgrupos de un grupo $\mathcal{G}$ y uno de ellos es invariante, entonces (*a*) $HK = KH$, (*b*) HK es un subgrupo de $\mathcal{G}$.

67. Demostrar: Si H y K son subgrupos invariantes de $\mathcal{G}$, también lo es HK.

68. Sean $\mathcal{G}$ con operación de grupo $\circ$ y elemento neutro u, y $\mathcal{G}'$ con operación de grupo $\square$ y elemento neutro u' dos grupos dados y fórmese

$$J = \mathcal{G} \times \mathcal{G}' = \{(g, g') : g \in \mathcal{G},\ g' \in \mathcal{G}'\}$$

Defínase el «producto» de pares de elementos $(g, g'), (h, h') \in J$ por

(*i*) $$(g, g')(h, h') = (g \circ h,\ g' \square h')$$

(*a*) Demostrar que J es un grupo respecto de la operación definida en (i).
(*b*) Demostrar que $S = \{(g, u') : g \in \mathcal{G}\}$ y $T = \{(u, g') : g' \in \mathcal{G}'\}$ son subgrupos de J.
(*c*) Demostrar que las aplicaciones

$$S \to \mathcal{G}\colon\ (g, u') \to g \quad \text{y} \quad T \to \mathcal{G}'\colon\ (u, g') \to g'$$

son isomorfismos.

69. Para $\mathcal{G}$ y $\mathcal{G}'$ del Problema 68, defínase $U = \{u\}$ y $U' = \{u'\}$. Asimismo, $\bar{\mathcal{G}} = \mathcal{G} \times U'$ y $\bar{\mathcal{G}}' = U \times \mathcal{G}'$. Demostrar:
(*a*) $\bar{\mathcal{G}}$ y $\bar{\mathcal{G}}'$ son subgrupos invariantes de J.
(*b*) $J/\bar{\mathcal{G}}$ es isomorfo a $U \times \mathcal{G}'$ y $J/\bar{\mathcal{G}}'$ a $\mathcal{G} \times U'$.
(*c*) $\bar{\mathcal{G}}$ y $\bar{\mathcal{G}}'$ tienen solamente (u, u') en común.
(*d*) Todo elemento de $\bar{\mathcal{G}}$ conmuta con todo elemento de $\bar{\mathcal{G}}'$.
(*e*) Todo elemento de J se puede expresar de manera única como producto de un elemento de $\bar{\mathcal{G}}$ por un elemento de $\bar{\mathcal{G}}'$.

70. Demostrar que S_4, A_4, $\{u, \rho^2, \sigma^2, \tau^2\}$, $\{u, \sigma^2\}$, U es una serie de composición de S_4. Hallar otra además de la del Ejemplo 13(*b*), página 90.

71. Para el grupo cíclico $\mathscr{G}$ de orden 36 generado por a:

(i) Demostrar que $a^2, a^3, a^4, a^6, a^9, a^{12}, a^{18}$, generan subgrupos invariantes $\mathscr{G}_{18}, \mathscr{G}_{12}, \mathscr{G}_9, \mathscr{G}_6, \mathscr{G}_4, \mathscr{G}_3, \mathscr{G}_2$, respectivamente, de $\mathscr{G}$.

(ii) $\mathscr{G}, \mathscr{G}_{18}, \mathscr{G}_9, \mathscr{G}_3, U$ es una serie de composición de $\mathscr{G}$. Hay seis series de composición de $\mathscr{G}$ en total; enumérense.

72. Demostrar el Teorema XXXII, página 91.

73. Escribir la tabla de operación para mostrar que $\bar{Q} = \{1, -1, i, -i, j, -j, k, -k\}$ con $i^2 = j^2 = k^2 = -1$, $ij = k = -ji, jk = i = -kj, ki = j = -ik$ forma un grupo.

74. Demostrar: Un grupo no conmutativo $\mathscr{G}$ con operación de grupo $\circ$ tiene al menos seis elementos.

Sugerencia: (1) $\mathscr{G}$ tiene a lo menos 3 elementos: el neutro, u, y dos elementos, a y b, que no conmutan.

(2) $\mathscr{G}$ tiene por lo menos 5 elementos: $u, a, b, a \circ b, b \circ a$. Supóngase que tiene solo 4. Entonces $a \circ b \neq b \circ a$ implica que $a \circ b$ o bien $b \circ a$ deben ser iguales a uno de los u, a, b.

(3) $\mathscr{G}$ tiene al menos 6 elementos $u, a, b, a \circ b, b \circ a$ y o bien a^2 o bien $a \circ b \circ a$.

75. Construir las tablas de operación para cada uno de los grupos no conmutativos de 6 elementos.

76. Considérese $S = \{u, a, a^2, a^3, b, ab, a^2b, a^3b\}$ con $a^4 = u$. Verificar:

(*a*) Si $b^2 = u$, entonces o bien $ba = ab$ o bien $ba = a^3b$. Escríbanse las tablas de operación A_8 cuando $ba = ab$ y D_8 cuando $ba = a^3b$ de los grupos que resultan.

(*b*) Si $b^2 = a$ o $b^2 = a^3$, los grupos que resultan son isomorfos a C_8, el grupo cíclico de orden 8.

(*c*) Si $b^2 = a^2$, entonces o bien $ba = ab$ o bien $ba = a^3b$. Escríbanse las tablas de operación A_8' cuando $ba = ab$ y Q_8 cuando $ba = a^3b$.

(*d*) A_8 y A_8' son isomorfos.

(*e*) D_8 es isomorfo al grupo octal.

(*f*) Q_8 es isomorfo al grupo $\bar{Q}$ (cuaternio) del Problema 73.

(*g*) Q_8 tiene solamente una serie de composición.

77. Obtener otro par de series de composición del grupo del Problema 19; establecer una biyección entre los grupos cocientes y escribir las aplicaciones por las que grupos cocientes correspondientes son isomorfos.

Capítulo 10

Anillos

ANILLOS

Se dice que un conjunto no vacío $\mathscr{R}$ forma anillo con respecto a las operaciones binarias de adición $(+)$ y multiplicación $(\cdot)$, si para cualesquiera $a, b, c \in \mathscr{R}$ se verifican las siguientes propiedades:

$\mathbf{P}_1$: $(a + b) + c = a + (b + c)$ (ley asociativa de la adición)

$\mathbf{P}_2$: $a + b = b + a$ (ley conmutativa de la adición)

$\mathbf{P}_3$: Existe un $z \in \mathscr{R}$ tal que $a + z = a$
(existencia de un neutro aditivo (el cero))

$\mathbf{P}_4$: Para todo $a \in \mathscr{R}$ existe $-a \in \mathscr{R}$ tal que $a + (-a) = z$
(existencia de simétricos aditivos)

$\mathbf{P}_5$: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (ley asociativa de la multiplicación)

$\mathbf{P}_6$: $a \cdot (b + c) = a \cdot b + a \cdot c$ (leyes distributivas)

$\mathbf{P}_7$: $(b + c) \cdot a = b \cdot a + c \cdot a$

Ejemplo 1: Dado que las propiedades enumeradas son solo unas cuantas de las propiedades comunes a Z, Q, R y C dotados de la adición y multiplicación ordinarias, se sigue que estos sistemas son ejemplos de anillos.

Ejemplo 2: El conjunto $S = \{x + y\sqrt[3]{3} + z\sqrt[3]{9};\ x, y, z \in Q\}$ es un anillo con respecto a la adición y multiplicación en R. Para probar esto, primero se demuestra que S es cerrado con respecto a estas operaciones. Se tiene para

$$a + b\sqrt[3]{3} + c\sqrt[3]{9},\ d + e\sqrt[3]{3} + f\sqrt[3]{9} \in S,$$

$$(a + b\sqrt[3]{3} + c\sqrt[3]{9}) + (d + e\sqrt[3]{3} + f\sqrt[3]{9}) = (a + d) + (b + e)\sqrt[3]{3} + (c + f)\sqrt[3]{9} \in S$$

y

$$(a + b\sqrt[3]{3} + c\sqrt[3]{9})(d + e\sqrt[3]{3} + f\sqrt[3]{9}) = (ad + 3bf + 3ce) + (ae + bd + 3cf)\sqrt[3]{3} + (af + be + cd)\sqrt[3]{9} \in S$$

Se ve en seguida que se cumplen P_1, P_2, P_5-P_7 puesto que S es un subconjunto del anillo R. Por último, $0 = 0 + 0\sqrt[3]{3} + 0\sqrt[3]{9}$ da cumplimiento a P_3 y para cada $x + y\sqrt[3]{3} + z\sqrt[3]{9} \in S$, existe $-x - y\sqrt[3]{3} - z\sqrt[3]{9} \in S$, lo cual cumple P_4. Así, pues, S tiene todos los requisitos de un anillo.

Ejemplo 3: (*a*) El conjunto $S = \{a, b\}$ con adición y multiplicación definidas por las tablas

$+$	a	b
a	a	b
b	b	a

y

$\cdot$	a	b
a	a	a
b	a	b

es un anillo.

(*b*) El conjunto $T = \{a, b, c, d\}$ con adición y multiplicación definidas por

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

y

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

es un anillo.

Para estos anillos el elemento cero es a y cada elemento es su propio simétrico aditivo.

Véanse también Problemas I-3.

En los Ejemplos 1 y 2 las operaciones binarias en los anillos (las operaciones de anillo) coinciden con la adición y multiplicación ordinarias en los distintos sistemas numéricos que intervienen; en el Ejemplo 3 carecen de significado fuera de las tablas dadas. En este ejemplo no puede haber confusión por el uso de símbolos familiares para denotar las operaciones de anillo. Sin embargo, cuando hay posibilidad de confusión, emplearemos los signos $\oplus$ y $\odot$ para indicar las operaciones de anillo.

Ejemplo 4: Considérese el conjunto de los números racionales Q. Es claro que $(\oplus)$ como adición y $(\odot)$ como multiplicación definidas por

$$a \oplus b = a \cdot b \quad \text{y} \quad a \odot b = a + b \quad \text{para cualesquiera } a, b \in Q$$

donde $+$ y $\cdot$ son la adición y multiplicación ordinarias con números racionales, son operaciones binarias sobre Q. Y se ve que $\mathbf{P}_1$, $\mathbf{P}_2$ y $\mathbf{P}_5$ se verifican de inmediato; asimismo, se verifica $\mathbf{P}_3$ con $z = 1$. Demuestre el lector que $\mathbf{P}_4$, $\mathbf{P}_6$ y $\mathbf{P}_7$ no se verifican y que, por tanto, Q no es anillo con respecto a $\oplus$ y $\odot$.

PROPIEDADES DE LOS ANILLOS

Las propiedades elementales de los anillos son análogas a las de Z, que no dependen ni de la ley conmutativa de la multiplicación ni de la existencia de un neutro multiplicativo. Anotamos algunas de estas propiedades:

(i) Todo anillo es un grupo aditivo abeliano.

(ii) Existe un elemento neutro aditivo *único*, z (el *cero* del anillo).
Véase Teorema III, Capítulo 2, página 20.

(iii) Cada elemento tiene un simétrico aditivo *único* (el *opuesto* de dicho elemento).
Véase Teorema IV, Capítulo 2, página 20.

(iv) Se cumple la ley de cancelación para la adición.

(v) $-(-a) = a$, $-(a + b) = (-a) + (-b)$ para cualesquiera a, b del anillo.

(vi) $a \cdot z = z \cdot a = z$. Para demostración, véase Problema 4.

(vii) $a \cdot (-b) = -(ab) = (-a) \cdot b$.

SUBANILLOS

Sea un anillo $\mathscr{R}$. Un subconjunto no vacío S del conjunto $\mathscr{R}$, que sea a su vez anillo respecto de las operaciones binarias de $\mathscr{R}$, se dice *subanillo* de $\mathscr{R}$. Si S es un subanillo de un anillo $\mathscr{R}$, es evidente que S es subgrupo del grupo aditivo $\mathscr{R}$.

Ejemplo 5: (*a*) Del Ejemplo 1 se sigue que Z es un subanillo de los anillos Q, R, C; que Q es un subanillo de R, C, y que R es un subanillo de C.

(*b*) En el Ejemplo 2, S es un subanillo de R.

(*c*) En el Ejemplo 3(*b*), $T_1 = \{a\}$, $T_2 = \{a, b\}$ son subanillos de T. ¿Por qué no es $T_3 = \{a, b, c\}$ subanillo de T?

Los subanillos $\{z\}$ y $\mathscr{R}$ mismo de un anillo $\mathscr{R}$ se dicen *impropios*, otros subanillos, si los hay en $\mathscr{R}$, se llaman *propios*.

Se deja al lector la demostración del

Teorema I. Sea $\mathscr{R}$ un anillo y sea S un subconjunto propio del conjunto $\mathscr{R}$. S es entonces un subanillo de $\mathscr{R}$ si, y solo si,

(*a*) S es cerrado respecto a las operaciones del anillo,

(*b*) para todo $a \in S$ se tiene $-a \in S$.

TIPOS DE ANILLOS

Un anillo en que la multiplicación sea conmutativa se llama anillo *conmutativo*.

Ejemplo 6: Los anillos de los Ejemplos 1, 2, 3(*a*) son conmutativos; el del Ejemplo 3(*b*) no es conmutativo, esto es $b \cdot c = a$, pero $c \cdot b = c$.

Un anillo dotado de elemento neutro multiplicativo (*elemento unidad*) se llama *anillo unitario*.

Ejemplo 7: Para cada uno de los anillos de los Ejemplos 1 y 2 la unidad es 1. La unidad del anillo del Ejemplo 3(*a*) es *b*; el anillo del Ejemplo 3(*b*) carece de unidad.

Sea $\mathscr{R}$ un anillo con unidad *u*. *u* es entonces su propio simétrico multiplicativo ($u^{-1} = u$), pero otros elementos no nulos de $\mathscr{R}$ pueden o no tener simétricos multiplicativos. Ahora bien, cuando los simétricos multiplicativos existen, son únicos.

Ejemplo 8: (*a*) El anillo del Problema 1 es un anillo no conmutativo sin unidad.

(*b*) El anillo del Problema 2 es un anillo conmutativo con unidad $u = h$. Aquí los elementos no nulos *b*, *e*, *f* no tienen simétricos multiplicativos; los simétricos de *c*, *d*, *g*, *h* son *g*, *d*, *c*, *h*, respectivamente.

(*c*) El anillo del Problema 3 tiene como unidad el $u = (1, 0, 0, 1)$. (Demuéstrese.) Como $(1, 0, 1, 0)(0, 0, 0, 1) = (0, 0, 0, 0)$ mientras que $(0, 0, 0, 1)(1, 0, 1, 0) = (0, 0, 1, 0)$, el anillo es no conmutativo. La existencia de simétricos multiplicativos se estudia en el Problema 5.

CARACTERISTICA

Sea $\mathscr{R}$ un anillo con elemento cero *z* y supóngase que existe un entero positivo *n* tal que $na = a + a + a + \cdots + a = z$ para todo $a \in \mathscr{R}$. El menor entero positivo *n* con tal propiedad se llama *característica* de $\mathscr{R}$. Si no existe un entero semejante, se dice que $\mathscr{R}$ tiene *característica cero*.

Ejemplo 9: (*a*) Los anillos *Z*, *Q*, *R*, *C* tienen característica cero, pues para estos anillos $na = n \cdot a$.

(*b*) En el Problema 1 se tiene $a + a = b + b = \cdots = h + h = a$, el cero del anillo, y la característica es entonces dos.

(*c*) El anillo del Problema 2 tiene característica cuatro.

DIVISORES DE CERO

Sea $\mathscr{R}$ un anillo con elemento cero *z*. Se dice que un elemento $a \neq z$ de $\mathscr{R}$ es un *divisor de cero*, si existe un elemento $b \neq z$ de $\mathscr{R}$ tal que $a \cdot b = z$ o bien $b \cdot a = z$.

Ejemplo 10: (*a*) Los anillos *Z*, *Q*, *R*, *C* no tienen divisores de cero, es decir, en cada sistema $ab = 0$ implica siempre o bien $a = 0$ o bien $b = 0$.

(*b*) Para el anillo del Problema 3 se vio en el Ejemplo 8(*c*) que $(1, 0, 1, 0)$ y $(0, 0, 0, 1)$ son divisores de cero.

(*c*) El anillo del Problema 2 tiene divisores de cero porque $b \cdot e = a$. Hallar todos los divisores de cero de este anillo.

HOMOMORFISMOS E ISOMORFISMOS

Un homomorfismo (isomorfismo) del grupo aditivo de un anillo $\mathscr{R}$ en (sobre) el grupo aditivo de un anillo $\mathscr{R}'$ que preserva también la segunda operación, la multiplicación, se llama homomorfismo (isomorfismo) de $\mathscr{R}$ en (sobre) $\mathscr{R}'$.

Ejemplo 11: Considérese el anillo $\mathscr{R} = \{a, b, c, d\}$ con tablas de adición y multiplicación

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

y el anillo $\mathscr{R}' = \{p, q, r, s\}$ con tablas de adición y multiplicación

+	p	q	r	s
p	r	s	p	q
q	s	r	q	p
r	p	q	r	s
s	q	p	s	r

·	p	q	r	s
p	s	p	r	q
q	p	q	r	s
r	r	r	r	r
s	q	s	r	p

La biyección

$$a \leftrightarrow r,\ b \leftrightarrow q,\ c \leftrightarrow s,\ d \leftrightarrow p$$

aplica $\mathscr{R}$ sobre $\mathscr{R}'$ (también $\mathscr{R}'$ sobre $\mathscr{R}$) preservando las operaciones binarias; por ejemplo,

$$d = b + c \leftrightarrow q + s = p$$

$$b = c \cdot d \leftrightarrow s \cdot p = q, \quad \text{etc.}$$

Así que $\mathscr{R}$ y $\mathscr{R}'$ son anillos isomorfos.

Utilizando los anillos isomorfos $\mathscr{R}$ y $\mathscr{R}'$ del Ejemplo 11, es fácil verificar el

Teorema II. En todo isomorfismo de un anillo $\mathscr{R}$ sobre un anillo $\mathscr{R}'$:

(*a*) si z es el cero de $\mathscr{R}$ y z' es el cero de $\mathscr{R}'$, se tiene $z \leftrightarrow z'$.

(*b*) si $\mathscr{R} \leftrightarrow \mathscr{R}'$: $a \leftrightarrow a'$, entonces $-a \leftrightarrow -a'$.

(*c*) si u es la unidad de $\mathscr{R}$ y u' es la unidad de $\mathscr{R}'$, se tiene $u \leftrightarrow u'$.

(*d*) si $\mathscr{R}$ es un anillo conmutativo, también lo es $\mathscr{R}'$.

IDEALES

Sea $\mathscr{R}$ un anillo con elemento cero z. Un subgrupo S de $\mathscr{R}$ que tiene la propiedad de que $r \cdot x \in S$ ($x \cdot r \in S$) para todo $x \in S$ y $r \in \mathscr{R}$, se llama *ideal a la izquierda* (*derecha*) de $\mathscr{R}$. Es claro que $\{z\}$ y $\mathscr{R}$ mismo son ambos ideales a izquierda y a derecha de $\mathscr{R}$; se les llama ideales *impropios* a la izquierda (derecha) de $\mathscr{R}$. Todos los demás ideales a la izquierda (derecha) de $\mathscr{R}$, si los hay, se llaman ideales *propios*.

Un subgrupo $\mathscr{I}$ de $\mathscr{R}$ que es ideal a la izquierda y a la derecha de $\mathscr{R}$, es decir, tal que para todo $x \in \mathscr{I}$ y $r \in \mathscr{R}$ se tiene $r \cdot x \in \mathscr{I}$ y $x \cdot r \in \mathscr{I}$, se llama *ideal* (*subanillo invariante*) de $\mathscr{R}$. Es claro que todo ideal a la izquierda (derecha) de un anillo conmutativo $\mathscr{R}$ es un ideal de $\mathscr{R}$.

Para todo anillo $\mathscr{R}$, los ideales $\{z\}$ y $\mathscr{R}$ mismo se llaman ideales *impropios* de $\mathscr{R}$, como ya se dijo, y todos los demás ideales de $\mathscr{R}$ se dicen *propios*. Un anillo que carece de ideales propios se llama anillo *simple*.

Ejemplo 12: (*a*) Para el anillo S del Problema 1, $\{a, b, c, d\}$ es un ideal propio a la derecha de S (examínense las primeras cuatro filas de la tabla de multiplicación), pero no es ideal a la izquierda (examínense las primeras cuatro columnas de la misma tabla). Los ideales propios de S son $\{a, c\}$, $\{a, e\}$, $\{a, g\}$ y $\{a, c, e, g\}$.

(*b*) En el anillo conmutativo Z, el subgrupo P de todos los múltiplos enteros de cualquier entero p es un ideal de Z.

(*c*) Para cualesquiera $a, b \in Q$ dados, el subgrupo $J = \{(ar, br, as, bs): r, s \in Q\}$ es un ideal a la izquierda del anillo M del Problema 3 y $K = \{(ar, as, br, bs): r, s \in Q\}$ es un ideal a la derecha de M porque para cualesquiera $(m, n, p, q) \in M$,

$$(m, n, p, q) \cdot (ar, br, as, bs] = \big(a(mr + ns),\ b(mr + ns),\ a(pr + qs),\ b(pr + qs)\big) \in J$$

y

$$(ar, as, br, bs) \cdot (m, n, p, q] = \big(a(mr + ps),\ a(nr + qs),\ b(mr + ps),\ b(nr + qs)\big) \in K$$

El Ejemplo 12(*b*) ilustra el

Teorema III. Si p es un elemento cualquiera de un anillo conmutativo $\mathscr{R}$, entonces $P = \{p \cdot r : r \in \mathscr{R}\}$ es un ideal de $\mathscr{R}$.

Para una demostración, véase Problema 9.

En el Ejemplo 12(*a*), cada elemento x del ideal a la izquierda $\{a, c, e, g\}$ tiene la propiedad de ser un elemento de S para el cual $r \cdot x = a$, el elemento cero de S, para todo $r \in S$. Esto ilustra el

Teorema IV. Sea $\mathscr{R}$ un anillo con elemento cero z; entonces

$$T = \{x : x \in \mathscr{R},\ r \cdot x = z\ (x \cdot r = z) \text{ para todo } r \in \mathscr{R}\}$$

es un ideal a la izquierda (derecha) de $\mathscr{R}$.

Sea $P, Q, S, T, \ldots$ una clase cualquiera de ideales de un anillo $\mathscr{R}$ y defínase $\mathscr{I} = P \cap Q \cap S \cap T \cap \cdots$. Como cada ideal de la clase es un grupo aditivo abeliano, entonces por el Teorema X, Capítulo 9, página 84, también lo es $\mathscr{I}$. Además, para todo $x \in \mathscr{I}$ y $r \in \mathscr{R}$, los productos $x \cdot r$ y $r \cdot x$ pertenecen a cada ideal de la clase y, por tanto, a $\mathscr{I}$. Hemos demostrado el

Teorema V. La intersección de cualesquiera ideales de un anillo es un ideal del anillo.

En el Problema 10 se demuestra

Teorema VI. En todo homomorfismo de un anillo $\mathscr{R}$ sobre otro anillo $\mathscr{R}'$, el conjunto S de elementos de $\mathscr{R}$ que se aplican sobre z', el elemento cero de $\mathscr{R}'$, es un ideal de $\mathscr{R}$.

Ejemplo 13: Considérese el anillo $G = \{a + bi : a, b \in Z\}$ del Problema 8.

(*a*) El conjunto de clases residuales módulo 2 de G es $H = \{[0], [1], [i], [1 + i]\}$. (Nótese que $1 + i \equiv 1 + i \pmod 2$.) De las tablas de operación para adición y multiplicación módulo 2, resulta que H es anillo conmutativo unitario; así, pues, H tiene divisores de cero aunque G no los tenga.

La aplicación $G \to H: g \to [g]$ es un homomorfismo en el cual $S = \{2g : g \in G\}$, ideal de G, se aplica sobre $[0]$, el elemento cero de H.

(*b*) El conjunto de clases residuales módulo 3 de G es

$$K = \{[0], [1], [i], [2], [2i], [1 + i], [2 + i], [1 + 2i], [2 + 2i]\}$$

Se puede demostrar como en (*a*) que K es un anillo conmutativo unitario, pero que no tiene divisores de cero.

IDEALES PRINCIPALES

Sea $\mathscr{R}$ un anillo y K un ideal a la derecha de $\mathscr{R}$ con la propiedad además

$$K = \{a \cdot r : r \in \mathscr{R},\ a \text{ es un elemento dado de } K\}$$

Se dirá entonces que K es *un ideal principal a la derecha* de $\mathscr{R}$ y que es generado por el elemento a de K. Análogamente se definen los ideales principales a la izquierda y los ideales principales.

Ejemplo 14: (*a*) En el anillo S del Problema 1 el subanillo $\{a, g\}$ es un ideal principal a la derecha de S generado por el elemento g (véase la fila de la tabla de multiplicación opuesta a g). Como $r \cdot g = a$ para todo $r \in S$ (véase la columna de la tabla de multiplicación encabezada g), $\{a, g\}$ no es ideal principal a la izquierda y, por tanto, no es ideal principal de S.

(*b*) En el anillo conmutativo S del Problema 2 el ideal $\{a, b, e, f\}$ de S es un ideal principal y se le puede considerar como generado por b, o por f.

(*c*) En el anillo S del Problema 1 el ideal a la derecha $\{a, b, c, d\}$ de S no es ideal principal a la derecha, pues no puede ser generado por ninguno de sus elementos.

(*d*) Para cualquier $m \in Z$, $J = \{mx : x \in Z\}$ es ideal principal de Z.

En el anillo Z, considérese el ideal principal K generado por el elemento 12. Es claro que K también es generado por el elemento -12. Como K no puede ser generado por ningún otro de sus elementos, defínase como ideal principal generado por 12. El generador 12 de K, además de ser un elemento de K, es también elemento de cada uno de los ideales principales: A generado por 6, B generado por 4, C generado por 3, D generado por 2 y Z mismo. Ahora bien, $K \subset A$, $K \subset B$, $K \subset C$, $K \subset D$, $K \subset Z$; además, 12 no pertenece a ningún otro ideal principal de Z. Así que K es la intersección de todos los ideales principales de Z que tienen a 12 entre sus elementos.

Se deduce de inmediato que cualquier ideal principal de Z generado por el entero m está contenido en todo ideal principal de Z generado por un factor de m. En particular, si m es primo, el único ideal principal de Z que contiene propiamente al ideal principal generado por m es Z.

Todo anillo $\mathscr{R}$ tiene al menos un ideal principal, a saber, el ideal *nulo* $\{z\}$ donde z es el elemento cero de $\mathscr{R}$. Todo anillo unitario tiene por lo menos dos ideales principales, a saber, $\{z\}$ y el ideal $\mathscr{R}$ generado por la unidad.

Sea $\mathscr{R}$ un anillo conmutativo. Si todo ideal de $\mathscr{R}$ es ideal principal, se dirá que $\mathscr{R}$ es un *anillo ideal principal*. Por ejemplo, considérese cualquier ideal $\mathscr{I} \neq \{0\}$ en el anillo de los enteros Z. Si $a \neq 0 \in \mathscr{I}$ también lo es $-a$. Luego $\mathscr{I}$ contiene enteros positivos y como Z^+ es bien ordenado, contiene un entero positivo mínimo, sea e. Para cualquier $b \in \mathscr{I}$ se tiene por el algoritmo de la división del Capítulo 5, página 50,

$$b = e \cdot q + r, \qquad q, r \in Z, \quad 0 \leq r < e$$

Pero $e \cdot q \in \mathscr{I}$; luego $r = 0$ y $b = e \cdot q$. Así, pues, $\mathscr{I}$ es un ideal principal de Z y hemos demostrado que

El anillo Z es un anillo ideal principal

IDEALES PRIMOS Y MAXIMALES

Se dice que un ideal $\mathscr{I}$ de un anillo conmutativo $\mathscr{R}$ es un *ideal primo*, si para elementos cualesquiera r, s de $\mathscr{R}$, $r \cdot s \in \mathscr{I}$ implica $r \in \mathscr{I}$ o bien $s \in \mathscr{I}$.

Ejemplo 15: En el anillo Z,

(*a*) El ideal $J = \{7r: r \in Z\}$, que también se escribe $J = (7)$, es un ideal primo porque si $a \cdot b \in J$ o bien $7 \mid a$ o bien $7 \mid b$; con lo que $a \in J$ o $b \in J$.

(*b*) El ideal $K = \{14r: r \in Z\}$ o $K = (14)$ no es ideal primo pues por ejemplo, $28 = 4 \cdot 7 \in K$ pero ni 4 ni 7 están en K.

El Ejemplo 15 ilustra el

Teorema VII. En el anillo Z un ideal propio $\mathscr{I} = \{mr: r \in Z, m \neq 0\}$ es un ideal primo si, y solamente si, m es un entero primo.

Un ideal propio $\mathscr{I}$ de un anillo conmutativo $\mathscr{R}$ se dice *maximal* si no hay en $\mathscr{R}$ ningún ideal propio que contenga propiamente a $\mathscr{I}$.

Ejemplo 16: (*a*) El ideal J del Ejemplo 15 es un ideal maximal de Z, puesto que el único ideal de Z que contiene propiamente a J es Z mismo.

(*b*) El ideal K del Ejemplo 15 no es ideal maximal porque K está contenido propiamente en J que, a su vez, está contenido propiamente en Z.

ANILLOS COCIENTES

Como el grupo aditivo de un anillo $\mathscr{R}$ es abeliano, todos sus subgrupos son subgrupos invariantes. Así que cualquier ideal $\mathscr{I}$ del anillo es un subgrupo invariante del grupo aditivo $\mathscr{R}$ y el grupo cociente $\mathscr{R}/\mathscr{I} = \{r + \mathscr{I}: r \in \mathscr{R}\}$ es el conjunto de todas las clases laterales distintas de $\mathscr{I}$ en $\mathscr{R}$.

(*Nota.* El empleo de $r + \mathscr{I}$ en vez del familiar $r\mathscr{I}$ para una clase lateral es en cierto sentido innecesario porque, por definición, $r\mathscr{I} = \{r \circ a: a \in \mathscr{I}\}$ y la operación *es* aquí la adición. Sin embargo, la usaremos.) En la sección Grupos cocientes del Capítulo 9, página 88, la adición (+) sobre las clases laterales (de un grupo aditivo) fue bien definida por

$$(x + \mathscr{I}) + (y + \mathscr{I}) = (x + y) + \mathscr{I}$$

Definimos ahora la multiplicación (·) sobre las clases laterales por

$$(x + \mathscr{I}) \cdot (y + \mathscr{I}) = (x \cdot y) + \mathscr{I}$$

y demostramos que también está bien definida. Para ello supóngase que $x' = x + s$ y $y' = y + t$ son elementos del grupo aditivo $\mathscr{R}$ tales que $x' + \mathscr{I}$ y $y' + \mathscr{I}$ son otras representaciones de $x + \mathscr{I}$ y $y + \mathscr{I}$, respectivamente. De

$$x' + \mathscr{I} = (x + s) + \mathscr{I} = (x + \mathscr{I}) + (s + \mathscr{I}) = x + \mathscr{I}$$

se sigue que s (y análogamente que t) $\in \mathscr{I}$. Entonces,

$$(x' + \mathscr{I}) \cdot (y' + \mathscr{I}) = (x' \cdot y') + \mathscr{I} = [(x \cdot y) + (x \cdot t) + (s \cdot y) + (s \cdot t)] + \mathscr{I} = (x \cdot y) + \mathscr{I}$$

puesto que $x \cdot t$, $s \cdot y$, $s \cdot t \in \mathscr{I}$ y la multiplicación está bien definida. (Hemos seguido llamando clase lateral a $x + \mathscr{I}$; en la teoría de anillos se la llama *clase residual* de $\mathscr{I}$ en el anillo $\mathscr{R}$.)

Ejemplo 17: Considérese el ideal $\mathscr{I} = \{3r: r \in Z\}$ del anillo Z en el grupo cociente $Z/\mathscr{I} = \{\mathscr{I}, 1 + \mathscr{I}, 2 + \mathscr{I}\}$. Es claro que los elementos de $Z/\mathscr{I}$ son simplemente las clases residuales de $Z/(3)$ y así, pues, constituyen un anillo con respecto a la adición y multiplicación módulo 3.

El Ejemplo 17 ilustra el

Teorema VIII. Si $\mathscr{I}$ es un ideal de un anillo $\mathscr{R}$, el grupo cociente $\mathscr{R}/\mathscr{I}$ es un anillo con respecto a la adición o multiplicación de clases laterales (clases residuales) según se acaban de definir.

Es costumbre designar este anillo por $\mathscr{R}/\mathscr{I}$ y llamarlo *anillo cociente* o *anillo factor* de $\mathscr{R}$ con respecto a $\mathscr{I}$.

De las definiciones de adición y multiplicación de clases residuales se sigue que

(*a*) La aplicación $\mathscr{R} \to \mathscr{R}/\mathscr{I}: a \to a + \mathscr{I}$ es un homomorfismo de $\mathscr{R}$ sobre $\mathscr{R}/\mathscr{I}$.

(*b*) $\mathscr{I}$ es el elemento cero del anillo $\mathscr{R}/\mathscr{I}$.

(*c*) Si $\mathscr{R}$ es un anillo conmutativo, también lo es $\mathscr{R}/\mathscr{I}$.

(*d*) Si $\mathscr{R}$ tiene elemento unidad u, también lo tiene $\mathscr{R}/\mathscr{I}$ y es $u + \mathscr{I}$.

(*e*) Si $\mathscr{R}$ carece de divisores de cero, $\mathscr{R}/\mathscr{I}$ puede o no tener divisores de cero. Pues, si bien

$$(a + \mathscr{I}) \cdot (b + \mathscr{I}) = a \cdot b + \mathscr{I} = \mathscr{I}$$

indica que $a \cdot b \in \mathscr{I}$, no implica necesariamente que $a \in \mathscr{I}$ o que $b \in \mathscr{I}$.

ANILLOS EUCLIDIANOS

En el capítulo siguiente trataremos de varios tipos de anillos; por ejemplo, de los anillos conmutativos, anillos unitarios, anillos sin divisores de cero, anillos conmutativos unitarios, . . . , que se obtienen añadiendo a las propiedades fundamentales del anillo una o más propiedades suplementarias (véase página 71) de $\mathscr{R}$. Hay otros tipos de anillos y vamos a terminar este capítulo con un breve estudio de uno de esos tipos que es de los *anillos euclidianos*:

Se llama anillo euclidiano cualquier anillo conmutativo $\mathscr{R}$ que tiene la propiedad de que a cada $x \in \mathscr{R}$ se le puede asignar un entero no negativo $\theta(x)$ tal que

(i) $\theta(x) = 0$ si, y solo si, $x = z$, el elemento cero de $\mathscr{R}$.

(ii) $\theta(x \cdot y) \geq \theta(x)$ si $x \cdot y \neq z$.

(iii) Para todo $x \in \mathscr{R}$ y $y \neq z \in \mathscr{R}$,

$$x = y \cdot q + r \qquad q, r \in \mathscr{R}, \quad 0 \leq \theta(r) < \theta(y)$$

Ejemplo 18: Z es un anillo euclidiano. Se ve fácilmente poniendo $\theta(x) = |x|$ para todo $x \in Z$.

Véase también Problema 12.

Se deduce también

Teorema IX Todo anillo euclidiano $\mathscr{R}$ es un anillo ideal principal.

Teorema X. Todo anillo euclidiano es unitario.

Problemas resueltos

1. El conjunto $S = \{a, b, c, d, e, f, g, h\}$ con adición y multiplicación definidas por

+	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	d	c	f	e	h	g
c	c	d	a	b	g	h	e	f
d	d	c	b	a	h	g	f	e
e	e	f	g	h	a	b	c	d
f	f	e	h	g	b	a	d	c
g	g	h	e	f	c	d	a	b
h	h	g	f	e	d	c	b	a

·	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b	a	b	a	b	a	b	a	b
c	a	c	a	c	a	c	a	c
d	a	d	a	d	a	d	a	d
e	a	e	a	e	a	e	a	e
f	a	f	a	f	a	f	a	f
g	a	g	a	g	a	g	a	g
h	a	h	a	h	a	h	a	h

es un anillo. La verificación exhaustiva de que se cumplen P_1 y P_5-P_7, página 101, es una tarea considerable, pero se encarece al lector hacer unas cuantas comprobaciones saltonas. El elemento cero es a y cada elemento es su propio simétrico aditivo.

2. El conjunto S del Problema 1 con adición y multiplicación definidas por

+	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	d	c	f	e	h	g
c	c	d	e	f	g	h	a	b
d	d	c	f	e	h	g	b	a
e	e	f	g	h	a	b	c	d
f	f	e	h	g	b	a	d	c
g	g	h	a	b	c	d	e	f
h	h	g	b	a	d	c	f	e

·	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b	a	e	f	b	a	e	f	b
c	a	f	d	g	e	b	h	c
d	a	b	g	h	e	f	c	d
e	a	a	e	e	a	a	e	e
f	a	e	b	f	a	e	b	f
g	a	f	h	c	e	b	d	g
h	a	b	e	d	e	f	g	h

es un anillo. ¿Cuál es el elemento cero? Hallar el simétrico aditivo de cada elemento.

3. Demostrar: El conjunto $M = \{(a, b, c, d): a, b, c, d \in Q\}$ con adición y multiplicación definidas por

$$(a, b, c, d) + (e, f, g, h) = (a + e, b + f, c + g, d + h)$$

$$(a, b, c, d)(e, f, g, h) = (ae + bg, af + bh, ce + dg, cf + dh)$$

para todo $(a, b, c, d), (e, f, g, h) \in M$ es un anillo.

Las leyes asociativa y conmutativa para la adición en el anillo son consecuencias inmediatas de las asociativa y conmutativa de la adición en Q. El elemento cero de M es $(0, 0, 0, 0)$ y el simétrico aditivo de (a, b, c, d) es $(-a, -b, -c, -d) \in M$. La ley asociativa para la multiplicación en el anillo se verifica como sigue:

$$\begin{aligned}
&[(a, b, c, d)(e, f, g, h)](i, j, k, l) \\
&\quad = \big((ae + bg)i + (af + bh)k,\ (ae + bg)j + (af + bh)l,\ (ce + dg)i + (ef + dh)k,\ (ce + dg)j + (ef + dh)l\big) \\
&\quad = \big(a(ei + fk) + b(gi + hk),\ a(ej + fl) + b(gj + hl),\ c(ei + fk) + d(gi + hk),\ c(ej + fl) + d(gj + hl)\big) \\
&\quad = (a, b, c, d)(ei + fk, ej + fl, gi + hk, gj + hl) \\
&\quad = (a, b, c, d)[(e, f, g, h)(i, j, k, l)]
\end{aligned}$$

para todo $(a, b, c, d), (e, f, g, h), (i, j, k, l) \in M$.

Los cálculos que se requieren para verificar las leyes distributivas se dejan al cuidado del lector.

4. Demostrar: Si $\mathscr{R}$ es un anillo con elemento cero z, entonces para todo $a \in \mathscr{R}$, $a \cdot z = z \cdot a = z$.

Como $a + z = a$, se sigue que

$$a \cdot a = (a + z)a = (a \cdot a) + z \cdot a$$

Como $a \cdot a = (a \cdot a) + z$; entonces, $(a \cdot a) + z \cdot a = (a \cdot a) + z$. Y utilizando la ley de cancelación, tenemos $z \cdot a = z$. Análogamente, $a \cdot a = a(a + z) = a \cdot a + a \cdot z$ y $a \cdot z = z$.

5. Investigar la posibilidad de que existan simétricos multiplicativos de elementos del anillo M del Problema 3.

Para cualquier elemento $(a, b, c, d) \neq (0, 0, 0, 0)$ de M hágase de

$$(a, b, c, d)(p, q, r, s) = (ap + br, aq + bs, cp + dr, cq + ds) = (1, 0, 0, 1)$$

la unidad de M y examínense las ecuaciones

$$\text{(i)} \quad \begin{cases} ap + br = 1 \\ cp + dr = 0 \end{cases} \qquad \text{(ii)} \quad \begin{cases} aq + bs = 0 \\ cq + ds = 1 \end{cases}$$

en cuanto a soluciones p, q, r, s.

Por (i) se tiene $(ad - bc)p = d$, así que siempre que $ad - bc \neq 0$, $p = \dfrac{d}{ad - bc}$ y $r = \dfrac{-c}{ad - bc}$. Análogamente, por (ii) se tiene que $q = \dfrac{-b}{ad - bc}$ y $s = \dfrac{a}{ad - bc}$. Se deduce que solamente aquellos elementos $(a, b, c, d) \in M$ para los que $ad - bc \neq 0$, poseen simétricos multiplicativos.

6. Demostrar que $P = \{(a, b, -b, a): a, b \in Z\}$ con adición y multiplicación definidas por

$$(a, b, -b, a) + (c, d, -d, c) = (a + c, b + d, -b - d, a + c)$$

y

$$(a, b, -b, a)(c, d, -d, c) = (ac - bd, ad + bc, -ad - bc, ac - bd)$$

es un subanillo conmutativo del anillo no conmutativo M del Problema 3.

Lo primero notamos que P es un subconjunto de M y que las operaciones definidas sobre P son precisamente las definidas sobre M. Ahora bien, P es cerrado respecto de estas operaciones; además, $(-a, -b, b, -a) \in P$ siempre que $(a, b, -b, a) \in P$. Así, pues, por el Teorema 1, P es un subanillo de M. Por último, para cualesquiera $(a, b, -b, a)$, $(c, d, -d, c) \in P$ se tiene

$$(a, b, -b, a)(c, d, -d, c) = (c, d, -d, c)(a, b, -b, a)$$

y P es un anillo conmutativo.

7. Considérese la aplicación $(a, b, -b, a) \to a$ del anillo P del Problema 6 en el anillo Z de los enteros.

El lector demostrará que la aplicación es tal que

$$(a, b, -b, a) + (c, d, -d, c) \to a + c$$

y

$$(a, b, -b, a) \cdot (c, d, -d, c) \to ac - bd$$

Pero los grupos aditivos de P y Z son homomorfos. (¿Por qué no isomorfos?) Sin embargo, como $ac - bd \neq ac$, en general, los anillos P y Z no son homomorfos por esta aplicación.

8. Un número complejo $a + bi$ con $a, b \in Z$ se llama *entero gaussiano*. (En el Problema 26 el lector ha de demostrar que el conjunto $G = \{a + bi: a, b \in Z\}$ de todos los enteros gaussianos es un anillo con respecto a la adición y multiplicación ordinarias sobre C.) Demuéstrese que el anillo P del Problema 6 y G son isomorfos.

Sea la aplicación $(a, b, -b, a) \to a + bi$ de P en G. La aplicación es ciertamente biyectiva y, además, como

$$(a, b, -b, a) + (c, d, -d, c) = (a + c, b + d, -b - d, a + c) \to (a + c) + (b + d)i = (a + bi) + (c + di)$$

y

$$(a, b, -b, a)(c, d, -d, c) = (ac - bd, ad + bc, -ad - bc, ac - bd) \to (ac - bd) + (ad + bc)i = (a + bi)(c + di)$$

todas las operaciones binarias se preservan. Así, pues, P y G son isomorfos.

9. Demostrar: Si p es un elemento cualquiera de un anillo conmutativo $\mathscr{R}$, entonces $P = \{p \cdot r: r \in \mathscr{R}\}$ es un ideal de $\mathscr{R}$.

Vamos a demostrar que P es un subgrupo del grupo aditivo $\mathscr{R}$ tal que $(p \cdot r) \cdot s \in P$ para todo $s \in \mathscr{R}$.

Para cualesquiera $r, s \in \mathscr{R}$, se tiene

(i) $p \cdot r + p \cdot s = p \cdot (r + s) \in P$, porque $r + s \in \mathscr{R}$; así, pues, P es cerrado con respecto a la adición.
(ii) $-(p \cdot r) = p \cdot (-r) \in P$ siempre que $p \cdot r \in P$ porque $-r \in \mathscr{R}$ si $r \in \mathscr{R}$; por el Teorema VII, Capítulo 9, página 84, P es un subgrupo del grupo aditivo.
(iii) $(p \cdot r) \cdot s = p \cdot (r \cdot s) \in P$ porque $(r \cdot s) \in \mathscr{R}$.

Y la demostración queda completa.

10. Demostrar: En todo homomorfismo de un anillo $\mathscr{R}$ con multiplicación denotada por $\cdot$, en otro anillo $\mathscr{R}'$ con multiplicación denotada por $\square$, el conjunto S de elementos de $\mathscr{R}$ que se aplican sobre z', el cero de $\mathscr{R}'$, es un ideal de $\mathscr{R}$.

Por el Teorema XXI, Capítulo 9, página 88, S es un subgrupo de $\mathscr{R}'$; luego para cualesquiera $a, b, c \in S$ se cumplen las propiedades $\mathbf{P}_1$-$\mathbf{P}_4$, página 101, y la adición del anillo es una operación binaria sobre S.

Como todos los elementos de S son elementos de $\mathscr{R}$ se verifican las propiedades $\mathbf{P}_5$-$\mathbf{P}_7$. Ahora bien, para cualesquiera $a, b \in S$, $a \cdot b \to z'$; luego $a \cdot b \in S$ y la multiplicación del anillo es una operación binaria sobre S.

Por último, para todo $a \in S$ y $g \in \mathscr{R}$ se tiene

$$a \cdot g \to z' \square g' = z' \quad \text{y} \quad g \cdot a \to g' \square z' = z'$$

Así que S es un ideal de $\mathscr{R}$.

11. Demostrar: El conjunto $\mathscr{R}/\mathscr{I} = \{r + \mathscr{I}: r \in \mathscr{R}\}$ de las clases laterales de un ideal $\mathscr{I}$ en un anillo $\mathscr{R}$ es él mismo un anillo con respecto a la adición y multiplicación definidas por

$$(x + \mathscr{I}) + (y + \mathscr{I}) = (x + y) + \mathscr{I}$$

y para todo $x + \mathscr{I}, y + \mathscr{I} \in R/\mathscr{I}$

$$(x + \mathscr{I}) \cdot (y + \mathscr{I}) = (x \cdot y) + \mathscr{I}$$

Como $\mathscr{I}$ es un subgrupo invariante del grupo $\mathscr{R}$, se sigue que $\mathscr{R}/\mathscr{I}$ es un grupo con respecto a la adición. Es claro por la definición de la multiplicación que se cumple la ley de clausura. Queda, pues, por demostrar que la ley asociativa y la distributiva se cumplen. Se encuentra para cualesquiera $w + \mathscr{I}$, $x + \mathscr{I}$, $y + \mathscr{I} \in \mathscr{R}/\mathscr{I}$,

$$\begin{aligned}[(w + \mathscr{I}) \cdot (x + \mathscr{I})] \cdot (y + \mathscr{I}) &= (w \cdot x + \mathscr{I}) \cdot (y + \mathscr{I}) = (w \cdot x) \cdot y + \mathscr{I} = w \cdot (x \cdot y) + \mathscr{I} \\ &= (w + \mathscr{I}) \cdot (x \cdot y + \mathscr{I}) = (w + \mathscr{I}) \cdot [(x + \mathscr{I}) \cdot (y + \mathscr{I})], \\ (w + \mathscr{I}) \cdot [(x + \mathscr{I}) + (y + \mathscr{I})] &= (w + \mathscr{I}) \cdot [(x + y) + \mathscr{I}] = [w \cdot (x + y)] + \mathscr{I} \\ &= (w \cdot x + w \cdot y) + \mathscr{I} = (w \cdot x + \mathscr{I}) + (w \cdot y + \mathscr{I}) \\ &= (w + \mathscr{I}) \cdot (x + \mathscr{I}) + (w + \mathscr{I}) \cdot (y + \mathscr{I})\end{aligned}$$

y, de manera parecida,

$$[(x + \mathscr{I}) + (y + \mathscr{I})] \cdot (w + \mathscr{I}) = (x + \mathscr{I}) \cdot (w + \mathscr{I}) + (y + \mathscr{I}) \cdot (w + \mathscr{I})$$

12. Demostrar: El anillo $G = \{a + bi: a, b \in Z\}$ es euclidiano.

Defínase $\theta(\alpha + \beta i) = \alpha^2 + \beta^2$ para todo $\alpha + \beta i \in G$. Se verifica fácilmente que las propiedades (i) y (ii), página 108, del anillo euclidiano se cumplen aquí. (Nótese también que $\theta(a + bi)$ es simplemente el cuadrado de la amplitud de $a + bi$ y que, por tanto, está definido para todos los elementos de C.)

Para todo $x \in G$ y $y \neq z \in G$ calcúlese $x \cdot y^{-1} = s + ti$. Ahora, si todo $s + ti \in G$, el teorema se seguiría fácilmente; no obstante, no es éste el caso, como el lector puede demostrar tomando $x = 1 + i$ y $y = 2 + 3i$.

Supóngase entonces para un x y un y dados que $s + ti \notin G$. Sea $c + di \in G$ tal que $|c - s| \leq \frac{1}{2}$ y $|d - t| \leq \frac{1}{2}$ y escríbase $x = y(c + di) + r$. Entonces, se tiene

$$\theta(r) = \theta[x - y(c + di)] = \theta[x - y(s + ti) + y(s + ti) - y(c + di)]$$
$$= \theta[y\{(s - c) + (t - d)i\}] \leq \tfrac{1}{2}\theta(y) < \theta(y)$$

Así, pues, se cumple (iii) y G es un anillo euclidiano.

Problemas propuestos

13. Demostrar que $S = \{2x: x \in Z\}$ con adición y multiplicación definidas como en Z, es un anillo, en tanto que $T = \{2x + 1: x \in Z\}$ no lo es.

14. Verificar que S del Problema 2 es un anillo conmutativo con unidad $= h$.

15. Con $a, b \in Z$ defínase $a \oplus b = a + b + 1$ y $a \odot b = a + b + ab$. Demostrar que Z es un anillo conmutativo con respecto a $\oplus$ y $\odot$. ¿Cuál es el cero de este anillo? ¿Tiene un elemento unidad?

16. Verificar que $S = \{a, b, c, d, e, f, g\}$ con adición y multiplicación definidas por

$+$	a	b	c	d	e	f	g
a	a	b	c	d	e	f	g
b	b	c	d	e	f	g	a
c	c	d	e	f	g	a	b
d	d	e	f	g	a	b	c
e	e	f	g	a	b	c	d
f	f	g	a	b	c	d	e
g	g	a	b	c	d	e	f

$\cdot$	a	b	c	d	e	f	g
a	a	a	a	a	a	a	a
b	a	b	c	d	e	f	g
c	a	c	e	g	b	d	f
d	a	d	g	c	f	b	e
e	a	e	b	f	c	g	d
f	a	f	d	b	g	e	c
g	a	g	f	e	d	c	b

es un anillo. ¿Cuál es la unidad? ¿Cuál la característica? ¿Tiene divisores de cero? ¿Es un anillo simple? Demostrar que es isomorfo al anillo $Z/(7)$.

17. Demostrar que $\bar{Q} = \{(z_1, z_2, -\bar{z}_2, \bar{z}_1): z_1, z_2 \in C\}$, con adición y multiplicación definidas como en el Problema 3, es un anillo no conmutativo con unidad $(1, 0, 0, 1)$. Verificar que cada elemento de $\bar{Q}$ con excepción del elemento cero $(z_1 = z_2 = 0 + 0i)$ tiene un simétrico multiplicativo o inverso de la forma $\{\bar{z}_1/\Delta, -z_2/\Delta, \bar{z}_2/\Delta, z_1/\Delta\}$ donde $\Delta = |z_1|^2 + |z_2|^2$ y que entonces los elementos no nulos de $\bar{Q}$ forman un grupo multiplicativo.

18. Demostrar que en todo anillo $\mathscr{R}$,

(*a*) $-(-a) = a$ para todo $a \in \mathscr{R}$

(*b*) $a(-b) = -(ab) = (-a)b$ para todos los $a, b \in \mathscr{R}$.

Sugerencia. (*a*) $a + [(-a) - (-a)] = a + z = a$

19. Considérese $\mathscr{R}$, el conjunto de todos los subconjuntos de un conjunto dado S y defínase para todos los $A, B \in \mathscr{R}$,

$$A \oplus B = A \cup B - A \cap B \qquad A \odot B = A \cap B$$

Demuéstrese que $\mathscr{R}$ es un anillo conmutativo unitario.

20. Demuéstrese que $S = \{(a, b, -b, a): a, b \in Q\}$ con adición y multiplicación definidas como en el Problema 6, es un anillo. ¿Cuál es el cero? ¿La unidad? ¿Es un anillo conmutativo? Procédase como en el Problema 5 para demostrar que todo elemento excepto $(0, 0, 0, 0)$ tiene un simétrico multiplicativo.

21. Completar las tablas de operación del anillo $\mathscr{R} = \{a, b, c, d\}$:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			a
d	a	b	c	

¿Es $\mathscr{R}$ un anillo conmutativo? ¿Tiene unidad? ¿Cuál es su característica?
Sugerencia. $c \cdot b = (b + d) \cdot b$; $c \cdot c = c \cdot (b + d)$; etc.

22. Completar las tablas de operación del anillo $\mathscr{R} = \{a, b, c, d\}$:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

	a	b	c	d
a	a	a	a	a
b	a	b		
c	a			c
d	a	b	c	

¿Es $\mathscr{R}$ un anillo conmutativo? ¿Tiene elemento unidad? ¿Cuál es su característica? Verificar que $x^2 = x$ para todo $x \in \mathscr{R}$. Un anillo que tiene esta propiedad se llama *anillo booliano*.

23. Demostrar: Si $\mathscr{R}$ es un anillo booliano, entonces (*a*) su característica es dos, (*b*) es un anillo conmutativo.
Sugerencia. Considérese $(x + y)^2 = x + y$ para $y = x$ y para $y \neq x$.

24. Sea $\mathscr{R}$ un anillo unitario y sean a y b elementos de $\mathscr{R}$ con inversos (simétricos multiplicativos) a^{-1} y b^{-1}, respectivamente. Demostrar que $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

25. Demostrar que $\{a\}$, $\{a, b\}$, $\{a, b, c, d\}$ son subanillos del anillo S del Problema 1.

26. Demostrar que $G = \{a + bi: a, b \in Z\}$, con respecto a la adición y multiplicación definidas sobre C, es un subanillo del anillo C.

27. Demostrar el Teorema 1, página 102.

28. (*a*) Verificar que $\mathscr{R} = \{(z_1, z_2, z_3, z_4): z_1, z_2, z_3, z_4 \in C\}$ con adición y multiplicación definidas como en el Problema 3, es un anillo con unidad $(1, 0, 0, 1)$. ¿Es anillo conmutativo?

(*b*) Demostrar que el subconjunto $S = \{(z_1, z_2, -z_2, z_1): z_1, z_2 \in C\}$ de $\mathscr{R}$ con adición y multiplicación definidas como en $\mathscr{R}$, es un subanillo de $\mathscr{R}$.

29. Enumerar todos los 15 subanillos de S del Problema 1.

30. Demostrar: Todo subanillo de un anillo $\mathscr{R}$ es un subgrupo del grupo aditivo $\mathscr{R}$.

31. Demostrar: Un subconjunto S de un anillo $\mathscr{R}$ es un subanillo de $\mathscr{R}$ si $a - b$ y $a \cdot b \in S$ siempre que $a, b \in S$.

32. Verificar que el conjunto $Z/(n)$ de los enteros módulo n es un anillo conmutativo unitario. ¿Cuándo el anillo carece de divisores de cero? ¿Cuál es la característica del anillo $Z/(5)$? ¿La del anillo $Z/(6)$?

33. Demostrar que el anillo $Z/(2)$ es isomorfo al anillo del Ejemplo 3(a).

34. Demostrar el Teorema II, página 104.

35. (a) Demostrar que $M_1 = \{(a, 0, c, d)\colon a, c, d \in Q\}$ y $M_2 = \{(a, 0, 0, d)\colon a, d \in Q\}$ con adición y multiplicación definidas como en el Problema 3, son subanillos de M del Problema 3.

(b) Demostrar que la aplicación $M_1 \to M_2\colon (x, 0, y, w) \to (x, 0, 0, w)$ es un isomorfismo.

(c) Demostrar que el subconjunto $\{(0, 0, y, 0)\colon y \in Q\}$ de elementos de M_1 que en (b) se aplican en $(0, 0, 0, 0) \in M_2$, es un ideal propio de M_1.

(d) Hallar un homomorfismo de M_1 en otro de sus subanillos y, como en (c), obtener otro ideal propio de M_1.

36. Demostrar: En todo homomorfismo de un anillo $\mathscr{R}$ sobre un anillo $\mathscr{R}'$ cuyo elemento neutro es z', sea

$$\mathscr{I} = \{x\colon x \in \mathscr{R},\ x \to z'\}$$

El anillo $\mathscr{R}/\mathscr{I}$ es entonces isomorfo al $\mathscr{R}'$.
Sugerencia. Considérese la aplicación $a + \mathscr{I} \to a'$ donde a' es la imagen de $a \in \mathscr{R}$ en el homomorfismo.

37. Sean a, b elementos conmutables de un anillo $\mathscr{R}$ de característica dos. Demostrar que $(a + b)^2 = a^2 + b^2 = (a - b)^2$.

38. Sea $\mathscr{R}$ un anillo con operaciones de anillo $+$ y $\cdot$, y $(a, r), (b, s) \in \mathscr{R} \times Z$. Demostrar que
(i) $\mathscr{R} \times Z$ es cerrado con respecto a la adición ($\oplus$) y a la multiplicación ($\odot$) definidas por

$$(a, r) \oplus (b, s) = (a + b, r + s)$$

$$(a, r) \odot (b, s) = (a \cdot b + rb + sa, rs)$$

(ii) $\mathscr{R} \times Z$ tiene $(z, 0)$ como cero y $(z, 1)$ como unidad.
(iii) $\mathscr{R} \times Z$ es un anillo con respecto a $\oplus$ y $\odot$.
(iv) $\mathscr{R} \times \{0\}$ es un ideal de $\mathscr{R} \times Z$.
(v) La aplicación $\mathscr{R} \leftrightarrow \mathscr{R} \times \{0\}\colon x \leftrightarrow (x, 0)$ es un isomorfismo.

39. Demostrar el Teorema IX, página 108. *Sugerencia*: Para todo ideal $\mathscr{I} \neq \{z\}$ de $\mathscr{R}$ elíjase el mínimo $\theta(y)$, sea $\theta(b)$, para todos los elementos no nulos $y \in \mathscr{I}$. Para todo $x \in \mathscr{I}$ escríbase $x = b \cdot q + r$ con $q, r \in \mathscr{I}$ y con $r = z$ o bien $\theta(r) < \theta(b)$.

40. Demostrar el Teorema X, página 108. *Sugerencia*: Supóngase que $\mathscr{R}$ es generado por a; entonces $a = a \cdot s = s \cdot a$ para algún $s \in \mathscr{R}$. Para cualquier $b \in \mathscr{R}$, $b = q \cdot a = q \cdot (a \cdot s) = b \cdot s$, etc.

Capítulo 11

Dominios de integridad, cuerpos

DOMINIOS DE INTEGRIDAD

Un anillo conmutativo unitario $\mathscr{D}$ sin divisores de cero se llama *dominio de integridad.*

Ejemplo 1: (*a*) Los anillos Z, Q, R y C son dominios de integridad.

(*b*) Los anillos de los Problemas 1 y 2, Capítulo 10, página 108, no son dominios de integridad, pues, por ejemplo, en ambos es $f \cdot e = a$, el cero del anillo.

(*c*) El conjunto $S = \{r + s\sqrt{17}:\ r, s \in Z\}$ con adición y multiplicación definidas como en R, es un dominio de integridad. Que S es cerrado con respecto a la adición y la multiplicación, resulta de

$$(a + b\sqrt{17}) + (c + d\sqrt{17}) = (a + c) + (b + d)\sqrt{17} \in S$$

$$(a + b\sqrt{17})(c + d\sqrt{17}) = (ac + 17bd) + (ad + bc)\sqrt{17} \in S$$

para cualesquiera $(a + b\sqrt{17}),\ (c + d\sqrt{17}) \in S$. Como S es un subconjunto de R, S carece de divisores de cero; y, además, se cumplen las leyes asociativas, conmutativas y distributivas. El cero de S es $0 \in R$ y todo $a + b\sqrt{17} \in S$ tiene simétrico aditivo, que es $-a - b\sqrt{17} \in S$. De modo que S es un dominio de integridad.

(*d*) El anillo $S = \{a, b, c, d, e, f, g, h\}$ con adición y multiplicación definidas por las tablas

+	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	a	d	c	f	e	h	g
c	c	d	a	b	g	h	e	f
d	d	c	b	a	h	g	f	e
e	e	f	g	h	a	b	c	d
f	f	e	h	g	b	a	d	c
g	g	h	e	f	c	d	a	b
h	h	g	f	e	d	c	b	a

·	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b	a	b	c	d	e	f	g	h
c	a	c	h	f	g	e	b	d
d	a	d	f	g	c	b	h	e
e	a	e	g	c	d	h	f	b
f	a	f	e	b	h	c	d	g
g	a	g	b	h	f	d	c	e
h	a	h	d	e	b	g	c	f

Tabla 11-1

es un dominio de integridad. Nótese que los elementos no nulos de S forman un grupo multiplicativo abeliano. Veremos luego que ésta es una propiedad común a los dominios de integridad finitos.

Aquí es necesaria una advertencia. El término dominio de integridad se emplea a veces por algunos para denotar cualquier anillo sin divisores de cero y por otros para cualquier anillo conmutativo sin divisores de cero.

Véase Problema 1.

La ley de cancelación para la adición resulta válida en todo dominio de integridad $\mathscr{D}$, pues todo elemento de $\mathscr{D}$ tiene simétrico aditivo. En el Problema 2 se demuestra que la ley de cancelación para la multiplicación se cumple también en $\mathscr{D}$ si bien los elementos no nulos de $\mathscr{D}$ no tienen necesariamente simétricos multiplicativos. En consecuencia, «carecer de divisores de cero» en la definición del dominio de integridad se puede cambiar por «verificarse la ley de cancelación para la multiplicación».

En el Problema 3 se demuestra el

Teorema I. Sea $\mathscr{D}$ un dominio de integridad e $\mathscr{I}$ un ideal de $\mathscr{D}$. Entonces $\mathscr{D}/\mathscr{I}$ es un dominio de integridad si, y solo si, $\mathscr{I}$ es ideal primo en $\mathscr{D}$.

ELEMENTOS INVERSIBLES, ASOCIADOS, DIVISORES

Sea $\mathscr{D}$ un dominio de integridad. Un elemento v de $\mathscr{D}$ que tenga simétrico multiplicativo o inverso en $\mathscr{D}$ se dice *inversible* o *regular* de $\mathscr{D}$. Un elemento b de $\mathscr{D}$ se dice *asociado* de $a \in \mathscr{D}$ si $b = v \cdot a$ siendo v un elemento inversible de $\mathscr{D}$.

Ejemplo 2: (*a*) Los únicos elementos inversibles de Z son ± 1; los únicos asociados de $a \in Z$ son $\pm a$.

(*b*) Considérese el dominio de integridad $\mathscr{D} = \{r + s\sqrt{17} : r, s \in Z\}$. Pues $\alpha = a + b\sqrt{17} \in \mathscr{D}$, es inversible si, y solo si, existe $x + y\sqrt{17} \in \mathscr{D}$ tal que

$$(a + b\sqrt{17})(x + y\sqrt{17}) = (ax + 17by) + (bx + ay)\sqrt{17} = 1 = 1 + 0\sqrt{17}$$

De $\begin{cases} ax + 17by = 1 \\ bx + ay = 0 \end{cases}$ se obtiene $x = \dfrac{a}{a^2 - 17b^2}$ y $y = \dfrac{-b}{a^2 - 17b^2}$. Como $x + y\sqrt{17} \in \mathscr{D}$, esto es, $x, y \in Z$ si, y solo si, $a^2 - 17b^2 = \pm 1$; luego α es inversible si, y solo si, $a^2 - 17b^2 = \pm 1$. Así, $\pm 1, 4 \pm \sqrt{17}, -4 \pm \sqrt{17}$ son elementos inversibles en $\mathscr{D}$ en tanto que $2 - \sqrt{17}$ y $-9 - 2\sqrt{17} = (2 - \sqrt{17})(4 + \sqrt{17})$ son asociados en $\mathscr{D}$.

(*c*) Todo elemento no nulo de $Z/(7) = \{0, 1, 2, 3, 4, 5, 6\}$ es elemento inversible de $Z/(7)$ ya que $1 \cdot 1 \equiv 1 \pmod 7$, $2 \cdot 4 \equiv 1 \pmod 7$, etc.

Véase Problema 4.

Un elemento a de $\mathscr{D}$ es un *divisor* de $b \in \mathscr{D}$ si existe un elemento c de $\mathscr{D}$ tal que $b = a \cdot c$. Todo elemento no nulo b de $\mathscr{D}$ tiene como divisores sus asociados en $\mathscr{D}$ y los inversibles de $\mathscr{D}$. Estos divisores se llaman *triviales* (*impropios*); todos los otros divisores, si los hay, se dicen *no triviales* (*propios*). Un elemento no nulo no inversible b de $\mathscr{D}$, que solo tiene divisores triviales, se llama *primo* (*elemento irreducible*) en $\mathscr{D}$. Un elemento b de $\mathscr{D}$, que tiene divisores no triviales, se dice elemento *reducible* de $\mathscr{D}$. Por ejemplo, 15 tiene divisores no triviales en Z, pero no en Q; 7 es primo en Z, pero no en Q.

Véase Problema 5.

Se sigue el

Teorema II. Si $\mathscr{D}$ es un dominio de integridad que también es anillo euclidiano, entonces para $a \neq z$, $b \neq z$ de $\mathscr{D}$,

$$\delta(a \cdot b) = \delta(a) \quad \text{si, y solo si, } b \text{ es inversible en } \mathscr{D}$$

SUBDOMINIOS

Un subconjunto $\mathscr{D}'$ de un dominio de integridad $\mathscr{D}$, que es, a su vez, un dominio de integridad con respecto a las operaciones de anillo de $\mathscr{D}$, se dice un *subdominio* de $\mathscr{D}$. Se deja al cuidado del lector demostrar que z y u, el cero y el elemento unidad de $\mathscr{D}$, son también los elementos cero y unidad de cualquier subdominio de $\mathscr{D}$.

Uno de los más interesantes subdominios de un dominio de integridad $\mathscr{D}$ (véase Problema 6) es

$$\mathscr{D}' = \{nu : n \in Z\}$$

donde nu tiene el mismo significado que en el Capítulo 10. Pues si $\mathscr{D}''$ fuese otro subdominio de $\mathscr{D}$, entonces $\mathscr{D}'$ sería un subdominio de $\mathscr{D}''$ y, por tanto, según la inclusión, $\mathscr{D}'$ es el *mínimo* subdominio de $\mathscr{D}$. Así, pues,

Teorema III. Si $\mathscr{D}$ es un dominio de integridad, el subconjunto $\mathscr{D}' = \{nu : n \in Z\}$ es su mínimo subdominio.

Por *característica* de un dominio de integridad $\mathscr{D}$ se entiende la característica del anillo $\mathscr{D}$ definida en el Capítulo 10. Los dominios de integridad del Ejemplo 1(*a*) son, pues, de característica cero, pero el del Ejemplo 1(*d*) tiene característica dos. En el Problema 7 se demuestra el

Teorema IV. La característica de un dominio de integridad es cero o un primo.

Sea $\mathscr{D}$ un dominio de integridad y su mínimo subdominio $\mathscr{D}'$ y sea la aplicación

$$Z \to \mathscr{D}' \colon n \to nu$$

Si $\mathscr{D}$ tiene característica cero, la aplicación es un isomorfismo de Z sobre $\mathscr{D}'$; luego podemos remplazar siempre $\mathscr{D}'$ por Z en $\mathscr{D}$. Si $\mathscr{D}$ es de característica p (un primo), la aplicación

$$Z/(p) \to \mathscr{D}' \colon [n] \to nu$$

es un isomorfismo de $Z/(p)$ sobre $\mathscr{D}'$.

DOMINIOS DE INTEGRIDAD ORDENADOS

Se llama *dominio de integridad ordenado* un dominio de integridad $\mathscr{D}$ que contiene un subconjunto $\mathscr{D}^+$ dotado de las propiedades:

(i) $\mathscr{D}^+$ es cerrado con respecto a la adición y multiplicación definidas sobre $\mathscr{D}$.

(ii) Para todo $a \in \mathscr{D}$ se verifica una, y solo una, de las relaciones

$$a = z \qquad a \in \mathscr{D}^+ \qquad -a \in \mathscr{D}^+$$

Los elementos de $\mathscr{D}^+$ se dicen elementos *positivos* de $\mathscr{D}$: todos los otros elementos no nulos de $\mathscr{D}$ se dicen elementos *negativos* de $\mathscr{D}$.

Ejemplo 3: Los dominios de integridad del Ejemplo 1(*a*) son dominios de integridad ordenados. En cada uno, el conjunto $\mathscr{D}^+$ consiste en los elementos positivos como se les definió en el capítulo en que apareció por primera vez el dominio.

Sea $\mathscr{D}$ un dominio de integridad ordenado y para cualesquiera $a, b \in \mathscr{D}$ defínase

$$a > b \quad \text{si} \quad a - b \in \mathscr{D}^+$$

y

$$a < b \quad \text{si, y solo si,} \quad b > a$$

como $a > z$ significa que $a \in \mathscr{D}^+$ y $a < z$ significa que $-a \in \mathscr{D}^+$, se sigue que si $a \neq z$, es entonces $a^2 \in \mathscr{D}^+$. En particular, $u \in \mathscr{D}^+$.

Supóngase ahora que $\mathscr{D}$ es un dominio de integridad ordenado con $\mathscr{D}^+$ bien ordenado; entonces u es el elemento mínimo de $\mathscr{D}^+$. Pues si hubiera un $a \in \mathscr{D}^+$ con $z < a < u$ entonces $z < a^2 < au = a$. Pero $a^2 \in \mathscr{D}^+$, de modo que $\mathscr{D}^+$ no tiene elemento mínimo en contradicción con lo dicho.

En el Problema 8 se demuestra el

Teorema V. Si $\mathscr{D}$ es un dominio de integridad ordenado con $\mathscr{D}^+$ bien ordenado, entonces

$$\text{(i)} \qquad \mathscr{D}^+ = \{pu\colon p \in Z^+\}$$

$$\text{(ii)} \qquad \mathscr{D} = \{mu\colon m \in Z\}$$

Por otra parte, la representación de cualquier $a \in \mathscr{D}$ como $a = mu$ es única.

Se deduce el

Teorema VI. Dos dominios de integridad ordenados $\mathscr{D}_1$ y $\mathscr{D}_2$ tales que sus respectivos conjuntos de elementos positivos $\mathscr{D}_1^+$ y $\mathscr{D}_2^+$ son bien ordenados, son isomorfos.

y el

Teorema VII. Aparte la notación, el anillo de los enteros Z es el único dominio de integridad ordenado cuyo conjunto de elementos positivos es bien ordenado.

ALGORITMO DE LA DIVISION

Sea $\mathscr{D}$ un dominio de integridad y supóngase que $d \in \mathscr{D}$ es un divisor común de los elementos no nulos $a, b \in \mathscr{D}$. Se dice que d es un *máximo común divisor* de a y b si para cualquier otro divisor común $d' \in \mathscr{D}$ se tiene $d' \mid d$. Si $\mathscr{D}$ es también un anillo euclidiano, $d' \mid d$ es equivalente a $\theta(d) > \theta(d')$.

(Para demostrar que esta definición concuerda con la de máximo común divisor de dos enteros tal como se dio en el Capitulo 5, supóngase que $\pm d$ son los máximos comunes divisores de $a, b \in Z$ y sea d' otro divisor común cualquiera. Como para $n \in Z$, $\theta(n) = |n|$ se sigue que $\theta(d) = \theta(-d)$ pero $\theta(d) > \theta(d')$.)

Para un dominio de integridad que sea a la vez anillo euclidiano se establece el

Algoritmo de la división. Sean $a \neq z$ y b elementos de $\mathscr{D}$ un dominio de integridad que también es anillo euclidiano. Existen entonces $q, r \in \mathscr{D}$ únicos, tales que

$$b = q \cdot a + r, \qquad 0 \leq \theta(r) < \theta(q)$$

Vèase Problema 5, Capitulo 5.

FACTORIZACION UNICA

En el Capitulo 5 se demostró que todo entero $a > 1$ se puede expresar de manera unívoca (aparte el orden de los factores) como producto de primos positivos. Supóngase que $a = p_1 \cdot p_2 \cdot p_3$ es una factorización semejante. Se tiene entonces

$$-a = -p_1 \cdot p_2 \cdot p_3 = p_1(-p_2)p_3 = p_1 \cdot p_2(-p_3) = (-1)p_1 \cdot p_2 \cdot p_3 = (-1)p_1 \cdot (-1)p_2 \cdot (-1)p_3$$

y esta factorización en factores *primos* se puede considerar como única aparte el empleo de elementos unidad como factores. Se puede, pues, enunciar otra vez el teorema de factorización única para los enteros como sigue:

Todo elemento no nulo y que no sea inversible de Z se puede expresar de manera única (aparte del orden de los factores y del empleo de elementos inversibles como factores) como producto de elementos primos de Z. En esta forma demostraremos luego que el teorema de factorización única vale en cualquier dominio de integridad que sea a la vez anillo euclidiano.

En el Problema 9 se demuestra el

Teorema VIII. Sean J y K, ambos distintos de $\{z\}$, ideales principales de un dominio de integridad $\mathscr{D}$. Entonces, $J = K$ si, y solo si, sus generadores son elementos asociados en $\mathscr{D}$.

En el Problema 10 se demuestra el

Teorema IX. Sean $a, b, p \in \mathscr{D}$ un dominio de integridad que también es anillo ideal principal, tales que $p \mid a \cdot b$. Entonces, si p es un elemento primo en $\mathscr{D}$, $p \mid a$ o bien $p \mid b$.

Una demostración de que el teorema de factorización única se cumple en un dominio de integridad que también sea anillo euclidiano (llamado también a veces dominio euclidiano) se da en el Problema 11.

Como consecuencia del Teorema IX, se tiene

Teorema X. En un dominio de integridad $\mathscr{D}$ en que sea válido el teorema de factorización única, todo elemento primo de $\mathscr{D}$ genera un ideal primo.

CUERPOS

Un anillo $\mathscr{S}$ cuyos elementos no nulos forman un grupo multiplicativo, se llama *cuerpo*. Todo cuerpo tiene un elemento unidad y todo elemento no nulo del cuerpo posee un inverso (simètrico multiplicativo); si la multiplicación es conmutativa, el cuerpo se dice conmutativo[1].

Ejemplo 4:
(*a*) Los anillos Q, R y C son cuerpos; y por ser conmutativa la multiplicación son cuerpos conmutativos.
(*b*) El anillo $\bar{Q}$ del Problema 17, Capitulo 10, es un cuerpo no conmutativo.
(*c*) El anillo Z no es cuerpo. (¿Por què?)

[1] Hay autores (principalmente en lengua inglesa) que llaman *anillos de división* o *seudocuerpos* (*Schiefkörper, skew fields*) a los cuerpos; y a èstos, cuando son conmutativos, les dicen *campos*. Nos atenemos a la nomenclatura más generalizada hoy en dia (Van der Waerden, Bourbaki). *N. del T.*

Sea $\mathscr{D}$ un dominio de integridad y su mínimo subdominio $\mathscr{D}'$ y sea la aplicación

$$Z \to \mathscr{D}' \colon n \to nu$$

Si $\mathscr{D}$ tiene característica cero, la aplicación es un isomorfismo de Z sobre $\mathscr{D}'$; luego podemos remplazar siempre $\mathscr{D}'$ por Z en $\mathscr{D}$. Si $\mathscr{D}$ es de característica p (un primo), la aplicación

$$Z/(p) \to \mathscr{D}' \colon [n] \to nu$$

es un isomorfismo de $Z/(p)$ sobre $\mathscr{D}'$.

DOMINIOS DE INTEGRIDAD ORDENADOS

Se llama *dominio de integridad ordenado* un dominio de integridad $\mathscr{D}$ que contiene un subconjunto $\mathscr{D}^+$ dotado de las propiedades:

(i) $\mathscr{D}^+$ es cerrado con respecto a la adición y multiplicación definidas sobre $\mathscr{D}$.

(ii) Para todo $a \in \mathscr{D}$ se verifica una, y solo una, de las relaciones

$$a = z \qquad a \in \mathscr{D}^+ \qquad -a \in \mathscr{D}^+$$

Los elementos de $\mathscr{D}^+$ se dicen elementos *positivos* de $\mathscr{D}$: todos los otros elementos no nulos de $\mathscr{D}$ se dicen elementos *negativos* de $\mathscr{D}$.

Ejemplo 3: Los dominios de integridad del Ejemplo 1(*a*) son dominios de integridad ordenados. En cada uno, el conjunto $\mathscr{D}^+$ consiste en los elementos positivos como se les definió en el capítulo en que apareció por primera vez el dominio.

Sea $\mathscr{D}$ un dominio de integridad ordenado y para cualesquiera $a, b \in \mathscr{D}$ defínase

$$a > b \quad \text{si} \quad a - b \in \mathscr{D}^+$$

y

$$a < b \quad \text{si, y solo si,} \quad b > a$$

como $a > z$ significa que $a \in \mathscr{D}^+$ y $a < z$ significa que $-a \in \mathscr{D}^+$, se sigue que si $a \neq z$, es entonces $a^2 \in \mathscr{D}^+$. En particular, $u \in \mathscr{D}^+$.

Supóngase ahora que $\mathscr{D}$ es un dominio de integridad ordenado con $\mathscr{D}^+$ bien ordenado; entonces u es el elemento mínimo de $\mathscr{D}^+$. Pues si hubiera un $a \in \mathscr{D}^+$ con $z < a < u$ entonces $z < a^2 < au = a$. Pero $a^2 \in \mathscr{D}^+$, de modo que $\mathscr{D}^+$ no tiene elemento mínimo en contradicción con lo dicho.

En el Problema 8 se demuestra el

Teorema V. Si $\mathscr{D}$ es un dominio de integridad ordenado con $\mathscr{D}^+$ bien ordenado, entonces

$$\text{(i)} \quad \mathscr{D}^+ = \{pu \colon p \in Z^+\}$$

$$\text{(ii)} \quad \mathscr{D} = \{mu \colon m \in Z\}$$

Por otra parte, la representación de cualquier $a \in \mathscr{D}$ como $a = mu$ es única.

Se deduce el

Teorema VI. Dos dominios de integridad ordenados $\mathscr{D}_1$ y $\mathscr{D}_2$ tales que sus respectivos conjuntos de elementos positivos $\mathscr{D}_1^+$ y $\mathscr{D}_2^+$ son bien ordenados, son isomorfos.

y el

Teorema VII. Aparte la notación, el anillo de los enteros Z es el único dominio de integridad ordenado cuyo conjunto de elementos positivos es bien ordenado.

ALGORITMO DE LA DIVISION

Sea $\mathscr{D}$ un dominio de integridad y supóngase que $d \in \mathscr{D}$ es un divisor común de los elementos no nulos $a, b \in \mathscr{D}$. Se dice que d es un *máximo común divisor* de a y b si para cualquier otro divisor común $d' \in \mathscr{D}$ se tiene $d' \mid d$. Si $\mathscr{D}$ es también un anillo euclidiano, $d' \mid d$ es equivalente a $\theta(d) > \theta(d')$.

(Para demostrar que esta definición concuerda con la de máximo común divisor de dos enteros tal como se dio en el Capítulo 5, supóngase que $\pm d$ son los máximos comunes divisores de $a, b \in Z$ y sea d' otro divisor común cualquiera. Como para $n \in Z$, $\theta(n) = |n|$ se sigue que $\theta(d) = \theta(-d)$ pero $\theta(d) > \theta(d')$.)

Para un dominio de integridad que sea a la vez anillo euclidiano se establece el

Algoritmo de la división. Sean $a \neq z$ y b elementos de $\mathscr{D}$ un dominio de integridad que también es anillo euclidiano. Existen entonces $q, r \in \mathscr{D}$ únicos, tales que

$$b = q \cdot a + r, \qquad 0 \leq \theta(r) < \theta(q)$$

Véase Problema 5, Capitulo 5.

FACTORIZACION UNICA

En el Capítulo 5 se demostró que todo entero $a > 1$ se puede expresar de manera univoca (aparte el orden de los factores) como producto de primos positivos. Supóngase que $a = p_1 \cdot p_2 \cdot p_3$ es una factorización semejante. Se tiene entonces

$$-a = -p_1 \cdot p_2 \cdot p_3 = p_1(-p_2)p_3 = p_1 \cdot p_2(-p_3) = (-1)p_1 \cdot p_2 \cdot p_3 = (-1)p_1 \cdot (-1)p_2 \cdot (-1)p_3$$

y esta factorización en factores *primos* se puede considerar como única aparte el empleo de elementos unidad como factores. Se puede, pues, enunciar otra vez el teorema de factorización única para los enteros como sigue:

Todo elemento no nulo y que no sea inversible de Z se puede expresar de manera única (aparte del orden de los factores y del empleo de elementos inversibles como factores) como producto de elementos primos de Z. En esta forma demostraremos luego que el teorema de factorización única vale en cualquier dominio de integridad que sea a la vez anillo euclidiano.

En el Problema 9 se demuestra el

Teorema VIII. Sean J y K, ambos distintos de $\{z\}$, ideales principales de un dominio de integridad $\mathscr{D}$. Entonces, $J = K$ si, y solo si, sus generadores son elementos asociados en $\mathscr{D}$.

En el Problema 10 se demuestra el

Teorema IX. Sean $a, b, p \in \mathscr{D}$ un dominio de integridad que también es anillo ideal principal, tales que $p \mid a \cdot b$. Entonces, si p es un elemento primo en $\mathscr{D}$, $p \mid a$ o bien $p \mid b$.

Una demostración de que el teorema de factorización única se cumple en un dominio de integridad que también sea anillo euclidiano (llamado también a veces dominio euclidiano) se da en el Problema 11.

Como consecuencia del Teorema IX, se tiene

Teorema X. En un dominio de integridad $\mathscr{D}$ en que sea válido el teorema de factorización única, todo elemento primo de $\mathscr{D}$ genera un ideal primo.

CUERPOS

Un anillo $\mathscr{S}$ cuyos elementos no nulos forman un grupo multiplicativo, se llama *cuerpo*. Todo cuerpo tiene un elemento unidad y todo elemento no nulo del cuerpo posee un inverso (simétrico multiplicativo); si la multiplicación es conmutativa, el cuerpo se dice conmutativo [1].

Ejemplo 4:
(*a*) Los anillos Q, R y C son cuerpos; y por ser conmutativa la multiplicación son cuerpos conmutativos.
(*b*) El anillo $\bar{Q}$ del Problema 17, Capítulo 10, es un cuerpo no conmutativo.
(*c*) El anillo Z no es cuerpo. (¿Por qué?)

[1] Hay autores (principalmente en lengua inglesa) que llaman *anillos de división* o *seudocuerpos* (*Schiefkörper, skew fields*) a los cuerpos; y a éstos, cuando son conmutativos, les dicen *campos*. Nos alenemos a la nomenclatura más generalizada hoy en día (Van der Waerden, Bonrbaki). *N. del T.*

Sea $\mathscr{D}$ un dominio de integridad con un número finito de elementos. Para todo $b \neq z \in \mathscr{D}$, se tiene

$$\{b \cdot x: x \in \mathscr{D}\} = \mathscr{D}$$

pues si no b seria divisor de cero. Asi que $b \cdot x = u$ para algún $x \in \mathscr{D}$ y b tiene inverso en $\mathscr{D}$. Queda así demostrado el

Teorema XI. Todo dominio de integridad con un número finito de elementos es un cuerpo conmutativo.

Demostremos ahora el

Teorema XII. Todo cuerpo es un anillo simple.

Supóngase que $\mathscr{I} \neq \{z\}$ sea un ideal de un cuerpo $\mathscr{S}$. Si $a \neq z \in \mathscr{I}$, se tiene $a^{-1} \in \mathscr{S}$ y $a \cdot a^{-1} = u \in \mathscr{I}$. Entonces, para todo $b \in \mathscr{S}$, $b \cdot u = b \in \mathscr{I}$; luego $\mathscr{I} = \mathscr{S}$.

Según ya se ha dicho, un cuerpo es conmutativo si los elementos no nulos forman grupo multiplicativo abeliano; y como todo cuerpo conmutativo es dominio de integridad, se deduce del Teorema IV, página 115, el

Teorema XIII. La característica de un cuerpo conmutativo es cero o es un número primo.

Todo subconjunto $\mathscr{F}'$ de un cuerpo $\mathscr{F}$, que es cuerpo a su vez, se llama *subcuerpo* del $\mathscr{F}$.

Ejemplo 5: Q es un subcuerpo de los cuerpos R y C; y R es también subcuerpo de C.

Véase también Problema 12.

Sea $\mathscr{F}$ un cuerpo de caracteristica cero. Su mínimo subdominio Z no es un subcuerpo. Pero como para todo $b \neq 0$, $b \in Z$, se tiene $b^{-1} \in \mathscr{F}$, se sigue que para cualesquiera $a, b \in Z$ con $b \neq 0$, $a \cdot b^{-1} = a/b \in \mathscr{F}$. Asi, pues, Q es el minimo subcuerpo de $\mathscr{F}$. Sea $\mathscr{F}$ un cuerpo de característica p prima. Entonces, $Z/(p)$, el minimo subdominio de $\mathscr{F}$ es el mínimo subcuerpo de $\mathscr{F}$.

Un cuerpo $\mathscr{F}$ que carece de subcuerpos propios $\mathscr{F}'$ se dice *cuerpo primo*. Q, por ejemplo, es el cuerpo primo de caracteristica cero y $Z/(p)$ es el cuerpo primo de caracteristica p, con p primo.

Enunciamos sin demostración el

Teorema XIV. Sea $\mathscr{F}$ un cuerpo primo. Si $\mathscr{F}$ tiene caracteristica cero es isomorfo a Q; si $\mathscr{F}$ tiene caracteristica p, siendo p primo, es isomorfo a $Z/(p)$.

En el Problema 13 se demuestra el

Teorema XV. Si $\mathscr{D}$ es un dominio de integridad e $\mathscr{I}$ es un ideal en $\mathscr{D}$, entonces $\mathscr{D}/\mathscr{I}$ es un cuerpo si, y solo si, $\mathscr{I}$ es un ideal maximal en $\mathscr{D}$.

Problemas resueltos

1. Demostrar: El anillo $Z/(m)$ es un dominio de integridad si, y solamente si, m es primo.

Supóngase que m es un primo p. Si $[r]$ y $[s]$ son elementos de $Z/(p)$ tales que $[r] \cdot [s] = [0]$, entonces $r \cdot s \equiv 0 (\text{mod } p)$ y $r \equiv 0 (\text{mod } p)$ o bien $s \equiv 0 (\text{mod } p)$. Luego $[r] = [0]$ o bien $[s] = [0]$ y como $Z/(p)$ carece de divisores de cero es, pues, un dominio de integridad.

Supóngase que m no es primo, es decir, que $m = m_1 \cdot m_2$ con $1 < m_1, m_2 < m$. Como $[m] = [m_1] \cdot [m_2] = [0]$, mientras que ni $[m_1] = [0]$ ni $[m_2] = [0]$, es evidente que $Z/(m)$ tiene divisores de cero y, por tanto, no es un dominio de integridad.

2. Demostrar: Para todo dominio de integridad se verifica la ley de cancelación de la multiplicación

$$\text{Si } a \cdot c = b \cdot c \text{ y } c \neq z, \text{ es } a = b$$

De $a \cdot c = b \cdot c$ se tiene $a \cdot c - b \cdot c = (a - b) \cdot c = z$. Como $\mathscr{D}$ no tiene divisores de cero, es $a - b = z$ y $a = b$, como se pedia.

3. Demostrar: Sean $\mathscr{D}$ un dominio de integridad e $\mathscr{I}$ un ideal de $\mathscr{D}$. Entonces, $\mathscr{D}/\mathscr{I}$ es un dominio de integridad si, y solamente si, $\mathscr{I}$ es un ideal primo en $\mathscr{D}$.

El caso $\mathscr{I} = \mathscr{D}$ es trivial; sea $\mathscr{I} \subset \mathscr{D}$.

Supóngase que $\mathscr{I}$ es un ideal primo en $\mathscr{D}$. Como $\mathscr{D}$ es un anillo conmutativo unitario, entonces también lo es $\mathscr{D}/\mathscr{I}$. Para demostrar que $\mathscr{D}/\mathscr{I}$ no tiene divisores de cero, supóngase que $a + \mathscr{I}, b + \mathscr{I} \in \mathscr{D}/\mathscr{I}$ son tales que

$$(a + \mathscr{I})(b + \mathscr{I}) = a \cdot b + \mathscr{I} = \mathscr{I}$$

Pero $a \cdot b \in \mathscr{I}$ y por definición de ideal primo o bien $a \in \mathscr{I}$ o bien $b \in \mathscr{I}$. Así, pues, es $a + \mathscr{I}$ o $b + \mathscr{I}$ el elemento cero de $\mathscr{D}/\mathscr{I}$. Y no teniendo $\mathscr{D}/\mathscr{I}$ divisores de cero es un dominio de integridad.

Recíprocamente, supóngase que $\mathscr{D}/\mathscr{I}$ es un dominio de integridad. Sean $a \neq z$ y $b \neq z$ de $\mathscr{D}$ tales que $a \cdot b \in \mathscr{I}$. De

$$\mathscr{I} = a \cdot b + \mathscr{I} = (a + \mathscr{I})(b + \mathscr{I})$$

se sigue que $a + \mathscr{I} = \mathscr{I}$ o bien que $b + \mathscr{I} = \mathscr{I}$. Así que $a \cdot b \in \mathscr{I}$ implica ya $a \in \mathscr{I}$, ya $b \in \mathscr{I}$, y, entonces, $\mathscr{I}$ es un ideal primo en $\mathscr{D}$.

Nota. Aunque $\mathscr{D}$ no tiene divisores de cero, esta propiedad no se ha utilizado en la demostración dada. De modo que en el teorema se puede remplazar «Sea $\mathscr{D}$ un dominio de integridad» por «Sea $\mathscr{R}$ un anillo unitario conmutativo».

4. Sea t un entero positivo que no es cuadrado perfecto y considérese el dominio de integridad $\mathscr{D} = \{r + s\sqrt{t}: r, s \in Z\}$. Para cada $\rho = r + s\sqrt{t} \in \mathscr{D}$ defínase $\bar{\rho} = r - s\sqrt{t}$ y la *norma* de ρ como $N(\rho) = \rho \cdot \bar{\rho}$. Del Ejemplo 2(*b*), página 115, inferimos que $\rho = a + b\sqrt{t}$ es inversible en $\mathscr{D}$ si, y solo si, $N(\rho) = \pm 1$. Demuéstrese que para $\alpha = a + b\sqrt{t} \in \mathscr{D}$ y $\beta = c + d\sqrt{t} \in \mathscr{D}$, $N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$.

Tenemos $\alpha \cdot \beta = (ac + bdt) + (ad + bc)\sqrt{t}$ y $\overline{\alpha \cdot \beta} = (ac + bdt) - (ad + bc)\sqrt{t}$. Entonces $N(\alpha \cdot \beta) = (\alpha \cdot \beta)(\overline{\alpha \cdot \beta}) = (ac + bdt)^2 - (ad + bc)^2 t = (a^2 - b^2 t)(c^2 - d^2 t) = N(\alpha) \cdot N(\beta)$, como se pedía.

5. En el dominio de integridad $\mathscr{D} = \{r + s\sqrt{17}: r, s \in Z\}$ verificar: (*a*) $9 - 2\sqrt{17}$ es un elemento primo, (*b*) $\gamma = 15 + 7\sqrt{17}$ es reducible.

(*a*) Supóngase $\alpha, \beta \in \mathscr{D}$ tales que $\alpha \cdot \beta = 9 - 2\sqrt{17}$. Por el Problema 4,

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) = N(9 - 2\sqrt{17}) = 13$$

Como 13 es un entero primo, o bien divide a $N(\alpha)$ o bien divide a $N(\beta)$; luego o bien es β o bien es α elemento inversible de $\mathscr{D}$, y $9 - 2\sqrt{17}$ es elemento primo.

(*b*) Supóngase $\alpha = a + b\sqrt{17}$, $\beta = c + d\sqrt{17} \in \mathscr{D}$ tales que $\alpha \cdot \beta = \gamma = 15 + 7\sqrt{17}$; entonces $N(\alpha) \cdot N(\beta) = -608$. De $N(\alpha) = a^2 - 17b^2 = 19$ y $N(\beta) = c^2 - 17d^2 = -32$, se obtiene $\alpha = 6 - \sqrt{17}$ y $\beta = 11 + 3\sqrt{17}$. Como ni α ni β son elementos inversibles de $\mathscr{D}$ ni asociados de γ, $15 + 7\sqrt{17}$ es reducible.

6. Demostrar que $\mathscr{D}' = \{nu: n \in Z\}$ donde u es la unidad de un dominio de integridad $\mathscr{D}$, es un subdominio de $\mathscr{D}$.

Para todo $ru, su \in \mathscr{D}'$ se tiene

$$ru + su = (r + s)u \in \mathscr{D}' \qquad \text{y} \qquad (ru)(su) = rsu \in \mathscr{D}'$$

luego $\mathscr{D}'$ es cerrado con respecto a las operaciones de anillo sobre $\mathscr{D}$. Asimismo,

$$0u = z \in \mathscr{D}' \qquad \text{y} \qquad 1u = u \in \mathscr{D}'$$

y para cada $ru \in \mathscr{D}'$ existe un simétrico aditivo $-ru \in \mathscr{D}'$. Por último $(ru)(su) = z$ implica $ru = z$ o bien $su = z$. Así que $\mathscr{D}'$ es un dominio de integridad, subdominio de $\mathscr{D}$.

7. Demostrar que la característica de un dominio de integridad $\mathscr{D}$ es cero o es prima.

En los Ejemplos 1(*a*) y 1(*d*) es evidente que hay dominios de integridad de característica cero y dominios de integridad de característica $m > 0$.

Supóngase que $\mathscr{D}$ tiene característica $m = m_1 \cdot m_2$ con $1 < m_1, m_2 < m$. Entonces $mu = (m_1 u)(m_2 u) = z$ y entonces o bien $m_1 u = z$ o bien $m_2 u = z$, que es una contradicción. Luego m es primo.

8. Demostrar: Si $\mathscr{D}$ es un dominio de integridad ordenado tal que $\mathscr{D}^+$ es bien ordenado, entonces

$$\text{(i)}\quad \mathscr{D}^+ = \{pu\colon p \in Z^+\} \qquad \text{(ii)}\quad \mathscr{D} = \{mu\colon m \in Z\}$$

Además, la representación de cualquier $a \in \mathscr{D}$ como $a = mu$ es única.

Como $u \in \mathscr{D}^+$ se sigue, por la propiedad de clausura, que $2u = u + u \in \mathscr{D}^+$ y, por inducción, que $pu \in \mathscr{D}^+$ para todo $p \in Z^+$. Denótese por E el conjunto de todos los elementos de $\mathscr{D}^+$ que no entran en el conjunto $\{pu : p \in Z^+\}$ y por e el elemento mínimo de E. Ahora bien, $u \notin E$, de modo que $e > u$ y, por tanto, $e - u \in \mathscr{D}^+$, pero $e - u \notin E$. (¿Por qué?). Entonces, $e - u = p_1 u$ para algún $p_1 \in Z^+$ y $e = u + p_1 u = (1 + p_1)u = p_2 u$, con $p_2 \in Z^+$. Pero esto es una contradicción; luego $E = \varnothing$ y queda establecido (i).

Supóngase $a \in \mathscr{D}$, pero $a \notin \mathscr{D}^+$; entonces, o bien $a = z$ o bien $-a \in \mathscr{D}^+$. Si $a = z$, es $a = 0u$. Si $-a \in \mathscr{D}^+$, entonces por (i), $-a = mu$ para algún $m \in Z^+$ de modo que $a = (-m)u$ y queda establecido (ii).

Es claro que si para cualquier $a \in \mathscr{D}$ se tiene $a = ru$ y $a = su$, donde $r, s \in Z$, entonces $z = a - a = ru - su = (r - s)u$ y $r = s$. Así que la representación de todo $a \in \mathscr{D}$ como $a = mu$ es única.

9. Demostrar: Sean J y K, cada uno distinto de $\{z\}$, ideales principales en un dominio de integridad $\mathscr{D}$. Entonces, $J = K$ si, y solamente si, sus generadores son elementos asociados en $\mathscr{D}$.

Sean a y b los generadores de J y K, respectivamente.

En primer lugar, supóngase que a y b son asociados y que $b = a \cdot v$ donde v es un elemento inversible en $\mathscr{D}$. Para cualquier $c \in K$ existe algún $s \in \mathscr{D}$ tal que

$$c = b \cdot s = (a \cdot v)s = a(v \cdot s) = a \cdot s', \qquad \text{con } s' \in \mathscr{D}$$

Entonces, $c \in J$ y $K \subseteq J$. Ahora bien, $b = a \cdot v$ implica $a = b \cdot v^{-1}$, así que, repitiendo el razonamiento con cualquier $d \in J$, se tiene $J \subseteq K$. Luego $J = K$ como se pedía.

Recíprocamente, supóngase que $J = K$. Entonces, para ciertos $s, t \in \mathscr{D}$ se tiene $a = b \cdot s$ y $b = a \cdot t$. Pero

$$a = b \cdot s = (a \cdot t)s = a(t \cdot s)$$

de manera que

$$a - a(t \cdot s) = a(u - t \cdot s) = z$$

donde u es el elemento unidad y z es el elemento cero de $\mathscr{D}$. Como $a \neq z$, por hipótesis, se tiene $u - t \cdot s = z$, de modo que $t \cdot s = u$ y s es un elemento inversible de $\mathscr{D}$. Así, pues, a y b son elementos asociados en $\mathscr{D}$ como se requería.

10. Demostrar: Sean $a, b, p \in \mathscr{D}$ un dominio de integridad que es también un anillo ideal principal, y supóngase $p \mid a \cdot b$. Entonces, si p es elemento primo en $\mathscr{D}$, $p \mid a$ o bien $p \mid b$.

Si uno de los a o b es inversible, o bien si a o b (o ambos) es un elemento asociado de p, el teorema es trivial. Supóngase lo contrario y, además, supóngase que $p \nmid a$. Denótese por $\mathscr{I}$ el ideal en $\mathscr{D}$ que es intersección de todos los ideales de $\mathscr{D}$ que contienen tanto a p como a a. Como $\mathscr{I}$ es un ideal principal, supóngase que es generado por $c \in \mathscr{I}$, de modo que $p = c \cdot x$ para algún $x \in \mathscr{D}$. Entonces o bien (i) x es inversible en $\mathscr{D}$ o bien (ii) c es inversible en $\mathscr{D}$.

(i) Supóngase que x es un elemento inversible en $\mathscr{D}$; entonces, por el Teorema VIII, p y su asociado c generan el mismo ideal principal $\mathscr{I}$. Como $a \in \mathscr{I}$, se tendrá

$$a = c \cdot g = p \cdot h \qquad \text{para ciertos } g, h \in \mathscr{D}$$

Pero entonces $p \mid a$, lo cual es contradictorio; luego x no es inversible.

(ii) Supóngase que c es inversible; entonces $c \cdot c^{-1} = u \in \mathscr{I}$ e $\mathscr{I} = \mathscr{D}$. Ahora bien, existen $s, t \in \mathscr{D}$ tales que $u = p \cdot s + t \cdot a$, donde u es la unidad de $\mathscr{D}$. Así que

$$b = u \cdot b = (p \cdot s)b + (t \cdot a)b = p(s \cdot b) + t(a \cdot b)$$

y como $p \mid a \cdot b$ se tiene $p \mid b$, como se afirmaba.

11. Demostrar: El teorema de factorización única es válido en todo dominio de integridad $\mathscr{D}$ que sea también anillo euclidiano.

Tenemos que demostrar que todo elemento no nulo, no inversible de $\mathscr{D}$, se puede expresar de manera única (excepto en el orden de los factores y en la aparición de elementos inversibles como factores) como producto de elementos primos de $\mathscr{D}$.

Suponiendo $a \neq 0 \in \mathscr{D}$ para el cual $\partial(a) = 1$, escríbase $a = b \cdot c$ no siendo b inversible; entonces c es inversible y a es un elemento primo en $\mathscr{D}$, pues si no

$$\partial(a) = \partial(b \cdot c) > \partial(b) \qquad \text{por el Teorema II, página 115}$$

Ahora aceptemos que el teorema sea válido para todo $b \in \mathscr{D}$ tal que $\partial(b) < m$ y considérese $c \in \mathscr{D}$, para el cual $\partial(c) = m$. Entonces, si c es elemento primo en $\mathscr{D}$, el teorema es válido para c. Supóngase, por el contrario, que c no es un elemento primo y escríbase $c = d \cdot e$, donde tanto d como e son divisores propios de c. Por el Teorema II se tiene, simultáneamente, $\partial(d) < m$ y $\partial(e) < m$. Por hipótesis, el teorema de factorización única es válido para d y para e, de modo que se verifica, por ejemplo,

$$c = d \cdot e = p_1 \cdot p_2 \cdot p_3 \cdots p_s$$

Como esta factorización de c resulta de la elección d, e de divisores propios, puede no ser única.

Supóngase que para otra elección de divisores propios se tuviera $c = q_1 \cdot q_2 \cdot q_3 \cdots q_t$. Considérese el factor primo p_1 de c. Por el Teorema IX, página 117, $p_1 \mid q_1$ o bien $p_1 \mid (q_2 \cdot q_3 \cdots q_t)$; si $p_1 \nmid q_1$, entonces $p_1 \mid q_2$ o bien $p_1 \mid (q_3 \cdots q_t)$; si ..... Supóngase $p_1 \mid q_j$. Entonces, $q_j = f \cdot p_1$, donde f es un elemento inversible en $\mathscr{D}$ porque si no q_j no sería un elemento primo en $\mathscr{D}$. Repitiendo el razonamiento con

$$p_2 \cdot p_3 \cdots p_s = f^{-1} \cdot q_1 \cdot q_2 \cdots q_{j-1} \cdot q_{j+1} \cdots q_t$$

se encuentra, por ejemplo, que $p_2 \mid q_k$, de modo que $q_k = g \cdot p_2$ con g elemento inversible en $\mathscr{D}$. Continuando de este modo, se encuentra, por último, aparte el orden de los factores y la aparición de elementos inversibles, que la factorización de c es única. Lo cual completa la demostración del teorema por inducción sobre m (véase Problema 27, Capítulo 3, página 37).

12. Demostrar: $S = \{x + y\sqrt[3]{3} + z\sqrt[3]{9} : x, y, z \in Q\}$ es un subcuerpo de R.

Por el Ejemplo 2, Capítulo 10, página 101, S es un subanillo del anillo R. Como la ley conmutativa se verifica en R y $1 = 1 + 0\sqrt[3]{3} + 0\sqrt[3]{9}$ es el neutro multiplicativo, es necesario únicamente verificar que para $x + y\sqrt[3]{3} + z\sqrt[3]{9} \neq 0 \in S$, el simétrico multiplicativo es $\frac{x^2 - 3yz}{D} + \frac{3z^2 - xy}{D}\sqrt[3]{3} + \frac{y^2 - xz}{D}\sqrt[3]{9}$, donde $D = x^3 + 3y^3 + 9z^3 - 9xyz$, está en S.

13. Demostrar: Sean $\mathscr{D}$ un dominio de integridad e $\mathscr{I}$ un ideal de $\mathscr{D}$. Entonces $\mathscr{D}/\mathscr{I}$ es un cuerpo si, y solo si, $\mathscr{I}$ es un ideal maximal de $\mathscr{D}$.

Primero supóngase que $\mathscr{I}$ es un ideal maximal de $\mathscr{D}$; luego $\mathscr{I} \subset \mathscr{D}$ y (véase Problema 3) $\mathscr{D}/\mathscr{I}$ es un anillo unitario conmutativo. Para demostrar que $\mathscr{D}/\mathscr{I}$ es un cuerpo, hay que demostrar que todo elemento no nulo tiene simétrico multiplicativo.

Para cualquier $q \in \mathscr{D} - \mathscr{I}$, considérese el subconjunto

$$S = \{a + q \cdot x : a \in \mathscr{I}, x \in \mathscr{D}\}$$

de $\mathscr{D}$. Para cualesquiera $y \in \mathscr{D}$ y $a + q \cdot x \in S$, se tiene $(a + q \cdot x) \cdot y = a' \cdot y + q(x \cdot y) \in S$ puesto que $a' \cdot y \in \mathscr{I}$; asimismo, $y \cdot (a + q \cdot x) \in S$. Así que S es un ideal de $\mathscr{D}$ y como $\mathscr{I} \subset S$, se tiene $S = \mathscr{D}$. De modo que todo $r \in \mathscr{D}$ se puede escribir $r = a + q \cdot e$ con $e \in \mathscr{D}$. Supóngase que para u, la unidad de $\mathscr{D}$, se tiene

$$u = a + q \cdot f, \qquad f \in \mathscr{D}$$

De

$$u + \mathscr{I} = (a + \mathscr{I}) + (q + \mathscr{I}) \cdot (f + \mathscr{I}) = (q + \mathscr{I}) \cdot (f + \mathscr{I})$$

se sigue que $f + \mathscr{I}$ es el simétrico multiplicativo de $q + \mathscr{I}$. Como q es un elemento cualquiera de $\mathscr{D} - \mathscr{I}$, el anillo de clases laterales $\mathscr{D}/\mathscr{I}$ es un cuerpo.

Recíprocamente, supóngase que $\mathscr{D}/\mathscr{I}$ es un cuerpo. Admitiremos que $\mathscr{I}$ no es maximal en $\mathscr{D}$ y llegaremos a una contradicción. Sea, pues J un ideal de $\mathscr{D}$ tal que $\mathscr{I} \subset J \subset \mathscr{D}$.

Para cualquier $a \in \mathscr{D}$ y cualquier $p \in J - \mathscr{I}$ definase $(p + \mathscr{I})^{-1} \cdot (a + \mathscr{I}) = s + \mathscr{I}$; entonces,

$$a + \mathscr{I} = (p + \mathscr{I}) \cdot (s + \mathscr{I})$$

Ahora, $a - p \cdot s \in \mathscr{I}$ y como $\mathscr{I} \subset J$, $a - p \cdot s \in J$. Pero $p \in J$; luego $a \in J$ y $J = \mathscr{D}$ en contradicción con $J \subset \mathscr{D}$. Así, pues, $\mathscr{I}$ es maximal en $\mathscr{D}$.

La nota al Problema 3, página 119, también se aplica aquí.

Problemas propuestos

14. Enumerar las propiedades que requiere un conjunto para ser un dominio de integridad.

15. Partiendo de la adición y la multiplicación definidas como para R, ¿cuáles de los conjuntos que siguen son dominios de integridad?

(*a*) $\{2a+1:\ a\in Z\}$ (*e*) $\{a+b\sqrt{3}:\ a,b\in Z\}$

(*b*) $\{2a:\ a\in Z\}$ (*f*) $\{r+s\sqrt{3}:\ r,s\in Q\}$

(*c*) $\{a\sqrt{3}:\ a\in Z\}$ (*g*) $\{a+b\sqrt{2}+c\sqrt{5}+d\sqrt{10}:\ a,b,c,d\in Z\}$

(*d*) $\{r\sqrt{3}:\ r\in Q\}$

16. Comprobar para el conjunto G de enteros gaussianos (véase Problema 8, Capitulo 10, página 110) que
(*a*) G es un dominio de integridad.
(*b*) $\alpha = a + bi$ es inversible si, y solo si, $N(\alpha) = a^2 + b^2 = 1$.
(*c*) Los únicos elementos inversibles son $\pm 1, \pm i$.

17. Definir $S = \{(a_1, a_2, a_3, a_4):\ a_i \in R\}$ con adición y multiplicación definidas, respectivamente, por

$$(a_1, a_2, a_3, a_4) + (b_1, b_2, b_3, b_4) = (a_1 + b_1,\ a_2 + b_2,\ a_3 + b_3,\ a_4 + b_4)$$

y

$$(a_1, a_2, a_3, a_4)(b_1, b_2, b_3, b_4) = (a_1 \cdot b_1,\ a_2 \cdot b_2,\ a_3 \cdot b_3,\ a_4 \cdot b_4)$$

Demostrar que S no es un dominio de integridad.

18. En el dominio de integridad $\mathscr{D}$ del Ejemplo 2(*b*), página 115, verificar que:

(*a*) $33 \pm 8\sqrt{17}$ y $-33 \pm 8\sqrt{17}$ son inversibles.

(*b*) $48 - 11\sqrt{17}$ y $879 - 92\sqrt{17}$ son asociados de $5 + 4\sqrt{17}$.

(*c*) $8 = 2\cdot 2\cdot 2 = 2(8 + 2\sqrt{17})(-8 + 2\sqrt{17}) = (5 + \sqrt{17})(5 - \sqrt{17})$, en donde cada factor es primo; luego la factorización única en primos no es una propiedad de $\mathscr{D}$.

19. Demostrar que la relación de asociación es una relación de equivalencia.

20. Demostrar que si para $\alpha \in \mathscr{D}$, $N(\alpha)$ es un entero primo, entonces α es un elemento primo de $\mathscr{D}$.

21. Demostrar que un anillo $\mathscr{R}$ dotado de la propiedad de que para cada $a \neq z, b \in \mathscr{R}$ existe un $r \in \mathscr{R}$ tal que $a \cdot r = b$, es un cuerpo.

22. Sean $\mathscr{D}' = \{[0], [5]\}$ y $\mathscr{D}'' = \{[0], [2], [4], [6], [8]\}$ subconjuntos de $\mathscr{D} = Z/(10)$. Demostrar:
(*a*) $\mathscr{D}'$ y $\mathscr{D}''$ son subdominios de $\mathscr{D}$.
(*b*) $\mathscr{D}'$ y $Z/(2)$ son isomorfos; y asimismo $\mathscr{D}''$ y $Z/(5)$ son isomorfos.
(*c*) Todo $a \in \mathscr{D}$ se puede escribir de manera única como $a = a' + a''$ donde $a' \in \mathscr{D}'$ y $a'' \in \mathscr{D}''$.
(*d*) Para $a, b \in \mathscr{D}$ con $a = a' + a''$ y $b = b' + b''$, $(a + b) = (a' + b') + (a'' + b'')$ y $a \cdot b = a' \cdot b' + a'' \cdot b''$.

23. Demostrar el Teorema 11.
Sugerencia. Si b es inversible, entonces $\theta(a) = \theta[b^{-1}(a \cdot b)] \geq \theta(a \cdot b)$. Si b no es inversible, considérese $a = q(a \cdot b) + r$ donde o bien es $r = z$ o bien $\theta(r) < \theta(a \cdot b)$ para $a \neq z \in \mathscr{D}$.

24. Demostrar que el conjunto S de todos los elementos inversibles de un dominio de integridad es un grupo multiplicativo.

25. Sean $\mathscr{D}$ un dominio de integridad de característica p y $\mathscr{D}' = \{x^p:\ x \in \mathscr{D}\}$. Demostrar:
(*a*) $(a \pm b)^p = a^p \pm b^p$ (*b*) La aplicación $\mathscr{D} \to \mathscr{D}':\ x \to x^p$ es un isomorfismo.

26. Demostrar que para todo $a \neq z, b$ de cualquier cuerpo, la ecuación $ax = b$ tiene una solución.

27. El conjunto $\mathcal{Q} = \{(q_1 + q_2 i + q_3 j + q_4 k)\colon q_1, q_2, q_3, q_4 \in R\}$ de *cuaternios* con adición y multiplicación definidas por

$$(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k) = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k$$

y

$$\begin{aligned}(a_1 + a_2 i + a_3 j + a_4 k) \cdot (b_1 + b_2 i + b_3 j + b_4 k) = {} & (a_1 b_1 - a_2 b_2 - a_3 b_3 - a_4 b_4) + (a_1 b_2 + a_2 b_1 + a_3 b_4 - a_4 b_3)i \\ & + (a_1 b_3 - a_2 b_4 + a_3 b_1 + a_4 b_2)j + (a_1 b_4 + a_2 b_3 - a_3 b_2 + a_4 b_1)k\end{aligned}$$

es un cuerpo no conmutativo. Demostrarlo. Comprobar que:

(*a*) Los subconjuntos $Q_2 = \{(q_1 + q_2 i + 0j + 0k)\}$, $Q_3 = \{(q_1 + 0i + q_3 j + 0k)\}$ y $Q_4 = \{(q_1 + 0i + 0j + q_4 k)\}$ de $\mathcal{Q}$ se combinan como el conjunto C de los números complejos; así, $i^2 = j^2 = k^2 = -1$.

(*b*) q_1, q_2, q_3, q_4 conmutan con i, j, k.

(*c*) $ij = k$, $jk = i$, $ki = j$

(*d*) $ji = -k$, $kj = -i$, $ik = -j$

(*e*) Con $\bar{Q}$ definido como en el Problema 17, Capítulo 10, página 111, la aplicación

$$\bar{Q} \to \mathcal{Q}\colon\ (q_1 + q_2 i, q_3 + q_4 i, -q_3 + q_4 i, q_1 - q_2 i) \to (q_1 + q_2 i + q_3 j + q_4 k)$$

es un isomorfismo.

(*f*) $\mathcal{Q}$ es un cuerpo no conmutativo (véase Ejemplo 4, página 117).

28. Demostrar que un cuerpo es un anillo conmutativo cuyos elementos no nulos poseen simétricos multiplicativos.

29. Demostrar que $P = \{(a, b, -b, a)\colon a, b \in R\}$ con adición y multiplicación definidas por

$$(a, b, -b, a) + (c, d, -d, c) = (a + c, b + d, -b - d, a + c)$$

y

$$(a, b, -b, a)(c, d, -d, c) = (ac - bd, ad + bc, -ad - bc, ac - bd)$$

es un cuerpo. Demostrar que P es isomorfo a C, el cuerpo de los números complejos.

30. (*a*) Demostrar que $\{a + b\sqrt{3}\colon a, b \in Q\}$ y $\{a + b\sqrt{2} + c\sqrt{6} + d\sqrt{10}\colon a, b, c, d \in Q\}$ son subcuerpos de R.

(*b*) Demostrar que $\{a + b\sqrt[3]{2}\colon a, b \in Q\}$ no es un subcuerpo de R.

31. Demostrar que $S = \{a + br\colon a, b \in R,\ r = -\frac{1}{2}(1 + \sqrt{3}\,i)\}$ es un subcuerpo de C.

Sugerencia. El simétrico multiplicativo de $a + br \neq 0 \in S$ es $\dfrac{a - b}{a^2 - ab + b^2} - \dfrac{b}{a^2 - ab + b^2} r \in S$.

32. (*a*) Demostrar que los subconjuntos $S = \{[0], [5], [10]\}$ y $T = \{[0], [3], [6], [9], [12]\}$ del anillo $Z/(15)$ son dominios de integridad con respecto a las operaciones binarias sobre $Z/(15)$.

(*b*) Demostrar que S es isomorfo a $Z/(3)$ y que, por tanto, es un cuerpo de característica 3.

(*c*) Demostrar que T es un cuerpo de característica 5.

33. Considérense los ideales $A = \{2g\colon g \in G\}$, $B = \{5g\colon g \in G\}$, $E = \{7g\colon g \in G\}$ y $F = \{(1 + i)g\colon g \in G\}$ de G, el anillo de los enteros gaussianos. (*a*) Demostrar que $G/A = G/(2)$ y que $G/B = G/(5)$ no son dominios de integridad. (*b*) Demostrar que G/E es un cuerpo de característica 7 y que G/F es un cuerpo de característica 2.

34. Demostrar que un cuerpo no contiene ideales propios.

35. Demostrar que los Problemas 3 y 13 implican que si $\mathcal{I}$ es un ideal maximal de un anillo unitario conmutativo $\mathcal{R}$ entonces $\mathcal{I}$ es un ideal primo de $\mathcal{R}$.

Capítulo 12

Polinomios

INTRODUCCION

Una gran parte del álgebra elemental trata de ciertos tipos de funciones como

$$1 + 2x + 3x^2 \qquad x + x^5 \qquad 5 - 4x^2 + 3x^{10}$$

llamadas polinomios en x. Los coeficientes en estos ejemplos son enteros, si bien no siempre es necesario que así sea. En el cálculo infinitesimal elemental, el dominio de definición de la función es R. En el álgebra tal dominio es C; por ejemplo, los valores de x para los cuales $1 + 2x + 3x^2$ es 0, son $-\frac{1}{3} \pm \frac{\sqrt{2}}{3}i$.

Desde el punto de vista del Capítulo 2, un polinomio en x se puede considerar como una aplicación de un conjunto S (dominio de x) sobre un conjunto T (dominio de valores del polinomio). Considérese, por ejemplo, el polinomio $1 + \sqrt{2}x - 3x^2$. Si $S = Z$, entonces $T \subset R$, y lo mismo ocurre si $S = Q$ o si $S = R$; si $S = C$, es entonces $T \subset C$.

Como en los capítulos precedentes, igualdad implica «idéntico a»; así dos polinomios en x son iguales si tienen idéntica forma. Por ejemplo, $a + bx = c + dx$ si, y solamente si, $a = c$ y $b = d$. (Nótese que $a + bx = c + dx$ nunca se ha de considerar aquí como una ecuación en x.)

Ya se sabe que las imágenes de cada valor de $x \in S$ son los mismos elementos de T cuando $\alpha(x) = \beta(x)$ y que, *en general*, son elementos distintos de T cuando $\alpha(x) \neq \beta(x)$. Sin embargo, como se verá en el Ejemplo 1 que sigue, esto depende en cierto modo del conjunto de x.

Ejemplo 1: Considérense los polinomios $\alpha(x) = [1]x$ y $\beta(x) = [1]x^5$, donde $[1] \in Z/(5)$, y supóngase que el dominio de definición sea el cuerpo $Z/(5) = \{[0], [1], [2], [3], [4]\}$. Es patente que $\alpha(x)$ y $\beta(x)$ difieren en forma (no son polinomios iguales); pero, como fácilmente se comprueba, las imágenes para cada $x \in Z/(5)$ son idénticas.

El Ejemplo 1 sugiere que en nuestro estudio de los polinomios empecemos por considerarlos como formas.

FORMAS POLINOMICAS

Sea $\mathscr{R}$ un anillo y sea x, que se llamará una *indeterminada*, un símbolo cualquiera que no pertenece a $\mathscr{R}$. Se entiende por *polinomio en x sobre $\mathscr{R}$* una expresión de la forma

$$\alpha(x) = a_0x^0 + a_1x^1 + a_2x^2 + \cdots = \sum a_kx^k, \qquad a_i \in \mathscr{R}$$

en la que solamente un número finito de las a son diferentes de z, el elemento cero de $\mathscr{R}$. Dos polinomios en x sobre $\mathscr{R}$, $\alpha(x)$ tal como se acaba de definir, y

$$\beta(x) = b_0x^0 + b_1x^1 + b_2x^2 + \cdots = \sum b_kx^k, \qquad b_i \in \mathscr{R}$$

se dicen *iguales*, $\alpha(x) = \beta(x)$, siempre que $a_k = b_k$ para todos los valores de k.

En todo polinomio tal como el $\alpha(x)$, cada uno de los componentes a_0x^0, a_1x^1, a_2x^2, . . . , se dice un *término*; en cada término a_ix^i, a_i se llama coeficiente del término. Aquí se han escrito los términos de $\alpha(x)$ y de $\beta(x)$ en un determinado orden (orden natural) y se hará así siempre. De modo que i, el superíndice de x, es apenas un indicador de la posición del término a_ix^i en el polinomio. Asimismo, la yuxtaposición de a_i y de x^i en el término a_ix^i no ha de interpretarse como indicación de multiplicación, y los signos más entre los términos se han de interpretar como medios de conexión más que como operadores. De hecho, bien pudiéramos haber escrito el polinomio $\alpha(x)$ anterior como $\alpha = (a_0, a_1, a_2, \ldots)$.

Si en un polinomio como $\alpha(x)$ el coeficiente $a_n \neq z$, en tanto que todos los coeficientes de los términos que siguen son z, se dice que $\alpha(x)$ es de *grado* n y a_n se llama coeficiente dominante. En particular, el polinomio $a_0x^0 + zx^1 + zx^2 + \ldots$ es de grado cero con coeficiente dominante a_0 cuando $a_0 \neq z$ y *no tiene grado* (ni *coeficiente dominante*) si $a_0 = z$.

Denotando por $\mathscr{R}[x]$ el conjunto de todos los polinomios en x sobre $\mathscr{R}$ y definiendo para cualesquiera $\alpha(x)$, $\beta(x) \in \mathscr{R}[x]$ la adición $(+)$ y la multiplicación $(\cdot)$ sobre $\mathscr{R}[x]$ por

$$\begin{aligned}\alpha(x) + \beta(x) &= (a_0 + b_0)x^0 + (a_1 + b_1)x^1 + (a_2 + b_2)x^2 + \cdots \\ &= \sum (a_k + b_k)x^k\end{aligned}$$

y

$$\begin{aligned}\alpha(x) \cdot \beta(x) &= a_0b_0x^0 + (a_0b_1 + a_1b_0)x^1 + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots \\ &= \sum c_kx^k, \quad \text{con} \quad c_k = \sum_0^k a_ib_{k-i}\end{aligned}$$

(Nótese que la multiplicación de elementos de $\mathscr{R}$ se indica aquí por yuxtaposición.)

Puede ser útil escribir completamente estas definiciones así:

$$\alpha(x) \boxplus \beta(x) = (a_0 \oplus b_0)x^0 + (a_1 \oplus b_1)x^1 + (a_2 \oplus b_2)x^2 + \cdots$$

y

$$\begin{aligned}\alpha(x) \boxdot \beta(x) &= (a_0 \odot b_0)x^0 + (a_0 \odot b_1 \oplus a_1 \odot b_0)x^1 \\ &\quad + (a_0 \odot b_2 \oplus a_1 \odot b_1 \oplus a_2 \odot b_0)x^2 + \cdots\end{aligned}$$

donde $\boxplus$ y $\boxdot$ son las nuevas operaciones definidas sobre $\mathscr{R}[x]$, $\oplus$ y $\odot$ son operaciones binarias sobre $\mathscr{R}$ y $+$ es como antes una conexión.

Es claro que tanto suma como producto de elementos de $\mathscr{R}[x]$ son elementos de $\mathscr{R}[x]$, es decir, solamente tienen un número finito de términos con coeficientes no nulos $\in \mathscr{R}$. Es fácil verificar que la adición sobre $\mathscr{R}[x]$ es asociativa y conmutativa y que la multiplicación es asociativa y distributiva con respecto a la adición. Además, el *polinomio cero*

$$zx^0 + zx^1 + zx^2 + \cdots = \sum zx^k \in \mathscr{R}[x]$$

es el *neutro aditivo* o *elemento cero* de $\mathscr{R}[x]$ y

$$-\alpha(x) = -a_0x^0 + (-a_1)x^1 + (-a_2)x^2 + \cdots = \sum (-a_k)x^k \in \mathscr{R}[x]$$

es el *simétrico aditivo* de $\alpha(x)$. Así, pues,

Teorema I. El conjunto de todos los polinomios $\mathscr{R}[x]$ en x sobre $\mathscr{R}$ es un anillo con respecto a la adición y multiplicación definidas anteriormente.

Sean $\alpha(x)$ y $\beta(x)$ de grados respectivos m y n. Si $m \neq n$, el grado de $\alpha(x) + \beta(x)$ es el mayor de los dos; si $m = n$ el grado de $\alpha(x) + \beta(x)$ es *a lo más* m (¿por qué?). El grado de $\alpha(x) \cdot \beta(x)$ es a lo más $m + n$ porque a_mb_n puede ser z. Sin embargo, si $\mathscr{R}$ no tiene divisores de cero, el grado del producto es $m + n$. (Siempre que sea conveniente seguiremos la costumbre de escribir un polinomio de grado m como uno de no más de $m + 1$ términos.)

Considérese el subconjunto $S = \{rx^0 : r \in \mathscr{R}\}$ de $\mathscr{R}[x]$ que consiste en el polinomio cero y en todos los polinomios de grado cero. Se comprueba fácilmente que la aplicación

$$\mathscr{R} \to S: \; r \to rx^0$$

es un isomorfismo. Por tanto, podemos escribir según esto a_0 en vez de a_0x^0 en cualquier polinomio $\alpha(x) \in \mathscr{R}[x]$.

POLINOMIOS MONICOS (UNITARIOS)†

Sea $\mathscr{R}$ un anillo con unidad u. Entonces $u = ux^0$ es la unidad de $\mathscr{R}[x]$ puesto que $ux^0 \cdot \alpha(x) = \alpha(x)$ para todo $\alpha(x) \in \mathscr{R}[x]$. Así que escribiendo $x = ux^1 = zx^0 + ux^1$, se tiene $x \in \mathscr{R}[x]$. Ahora bien, $a_k(x \cdot x \cdot x \cdots \text{con } k \text{ factores}) = a_kx^k \in \mathscr{R}[x]$ de modo que en $\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots$ podemos considerar el superíndice i en a_ix^i como un verdadero exponente, la yuxtaposición en cualquier término a_ix^i como multiplicación en el anillo (polinómica) y la conexión $+$ como adición en el anillo (polinómica).

Todo polinomio $\alpha(x)$ de grado m sobre $\mathscr{R}$ con coeficiente dominante u, la unidad de $\mathscr{R}$, se llamará *mónico* (o unitario).

Ejemplo 2: (*a*) Los polinomios $1, x + 3, x^2 - 5x + 4$ son mónicos, mientras que $2x^2 - x + 5$ no lo es, sobre Z (o sobre cualquier anillo que tenga a Z como subanillo).

(*b*) Los polinomios $b, bx + f$ y $bx^2 + dx + e$ son polinomios mónicos en $S[x]$ sobre el anillo S del Ejemplo 1(*d*), Capítulo 11, página 114.

DIVISION

En el Problema 1 se demuestra la primera parte del

Teorema II. Sean $\mathscr{R}$ un anillo con unidad u, $\alpha(x) = a_0 + a_1x^1 + a_2x^2 + \cdots + a_mx^m \in \mathscr{R}[x]$ bien el polinomio cero o bien un polinomio de grado m, y $\beta(x) = b_0 + b_1x_1 + b_2x^2 + \cdots + u_nx^n \in \mathscr{R}[x]$ un polinomio mónico de grado n. Existe un par de polinomios único $q_R(x)$, $r_R(x)$; $q_L(x)$, $r_L(x) \in \mathscr{R}[x]$ con $r_R(x)$, $r_L(x)$ polinomios cero o de grado $< n$ tales que

$$\text{(i)} \qquad \alpha(x) = q_R(x) \cdot \beta(x) + r_R(x)$$

y

$$\text{(ii)} \qquad \alpha(x) = \beta(x) \cdot q_L(x) + r_L(x)$$

En (i) del Teorema II se dice que $\alpha(x)$ se ha dividido *a la derecha* por $\beta(x)$ para obtener el *cociente a la derecha* $q_R(x)$ y el *resto a la derecha* $r_R(x)$. Análogamente, en (ii) se dice que $\alpha(x)$ se ha dividido a la izquierda por $\beta(x)$ para obtener el *cociente a la izquierda* $q_L(x)$ y el *resto a la izquierda* $r_L(x)$. Cuando $r_R(x) = z$ ($r_L(x) = z$), se dice que $\beta(x)$ es *divisor* a la derecha (a la izquierda) de $\alpha(x)$.

Para el caso especial $\beta(x) = ux - b = x - b$, el Teorema II da (véase Problema 2) el

Teorema III. Los restos a la derecha y a la izquierda cuando $\alpha(x)$ se divide por $x - b$, $b \in \mathscr{R}$, son respectivamente

$$r_R = a_0 + a_1b + a_2b^2 + \cdots + a_nb^n$$

y

$$r_L = a_0 + ba_1 + b^2a_2 + \cdots + b^na_n$$

De lo que se sigue el

Teorema IV. Un polinomio $\alpha(x)$ tiene a $x - b$ como divisor a la derecha (a la izquierda) si, y solo si, $r_R = z$ ($r_L = z$).

Ejemplos que ilustren los Teoremas II y IV cuando $\mathscr{R}$ no es conmutativo se postergan hasta el Capítulo 15. Lo que queda de este capítulo se dedica al estudio de ciertos anillos de polinomios $\mathscr{R}[x]$ que se obtienen especializando cada vez más el anillo de coeficientes $\mathscr{R}$.

† La denominación «unitario» dada a un polinomio de coeficiente dominante $a_n = u$ puede prestarse a confusión; se ha preferido mantener el neologismo «mónico». *N. del T.*

ANILLOS CONMUTATIVOS UNITARIOS DE POLINOMIOS

Sea $\mathscr{R}$ un anillo conmutativo unitario. Entonces $\mathscr{R}[x]$ es un anillo conmutativo unitario (¿cuál es su unidad?) y los Teoremas II y IV se pueden enunciar sin distinguir entre cocientes a la derecha y cocientes a la izquierda (se remplazan $q_R(x) = q_L(x)$ por $q(x)$), restos (se remplaza $r_R(x) = r_L(x)$ por $r(x)$) y divisores. Así (i) y (ii) del Teorema II se pueden remplazar por

$$\text{(iii)} \qquad \alpha(x) = q(x)\cdot\beta(x) + r(x)$$

y en particular, se tiene el

Teorema IV'. En un anillo conmutativo unitario de polinomios, un polinomio $\alpha(x)$ de grado m tiene a $x - b$ como divisor si, y solo si, el resto

$$(a) \qquad r = a_0 + a_1 b + a_2 b^2 + \cdots + a_m b^m = z$$

Cuando como en el Teorema IV', $r = z$ se dice que b es un *cero* (o *raíz*) del polinomio $\alpha(x)$.

Ejemplo 3:

(*a*) El polinomio $x^2 - 4$ sobre Z tiene 2 y -2 como ceros, puesto que $(2)^2 - 4 = 0$ y también $(-2)^2 - 4 = 0$.

(*b*) El polinomio $[3]x^2 - [4]$ sobre el anillo $Z/(8)$ tiene los ceros $[2]$ y $[6]$ mientras que el polinomio $[1]x^2 - [1]$ sobre $Z/(8)$ tiene como ceros a $[1], [3], [5], [7]$.

Si $\mathscr{R}$ no tiene divisores de cero, pasa igual con $\mathscr{R}[x]$. Porque supóngase que $\alpha(x)$ y $\beta(x)$ son elementos de $\mathscr{R}[x]$ de grados respectivos m y n, y que

$$\alpha(x)\cdot\beta(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + a_m b_n x^{m+n} = z$$

Entonces, cada coeficiente del producto, y en particular $a_m b_n$, es z. Pero $\mathscr{R}$ carece de divisores de cero; luego $a_m b_n = z$ si, y solo si, $a_m = z$ o si $b_n = z$. Como esto contradice la hipótesis de que $\alpha(x)$ y $\beta(x)$ eran de grados m y n, entonces $\mathscr{R}[x]$ no tiene divisores de cero.

Y se sigue entonces el

Teorema V. Un anillo de polinomios $\mathscr{R}[x]$ es dominio de integridad si, y solo si, el anillo $\mathscr{R}$ de los coeficientes es un anillo de integridad.

SUSTITUCION DE LA INDETERMINADA

Observando el resto

$$(a) \qquad r = a_0 + a_1 b + a_2 b^2 + \cdots + a_m b^m$$

en el Teorema IV' se ve que se le puede obtener mecánicamente sin más que remplazar x por b en el polinomio $\alpha(x)$ y naturalmente interpretando la yuxtaposición de elementos como multiplicación en $\mathscr{R}$. Así, pues, si se define $f(b)$ como la expresión que se obtiene sustituyendo x por b en $f(x)$, podemos remplazar (y así se hará) r en (*a*) por $\alpha(b)$. Cosa que no es más que el proceso familiar de sustitución del álgebra elemental («valor numérico») donde (obsérvese) x se considera como una variable más bien que como una indeterminada.

Se deja al cuidado del lector demostrar que el proceso de sustitución o de «dar valor numérico» no da lugar a dificultades posteriores, es decir, el demostrar que para un $b \in \mathscr{R}$ dado, la aplicación

$$f(x) \to f(b) \qquad \text{para todo} \qquad f(x) \in \mathscr{R}[x]$$

es un homomorfismo de $\mathscr{R}[x]$ sobre $\mathscr{R}$.

EL DOMINIO DE POLINOMIOS $\mathscr{F}[x]$

Los dominios polinómicos más importantes se tienen cuando el anillo de los coeficientes es un cuerpo $\mathscr{F}$. Recuérdese que todo elemento no nulo de un cuerpo $\mathscr{F}$ es inversible en $\mathscr{F}$; y volveremos a enunciar los principales resultados de las secciones anteriores para el dominio de integridad $\mathscr{F}[x]$ como sigue:

Algoritmo de la división. Si $\alpha(x), \beta(x) \in \mathscr{F}[x]$ con $\beta(x) \neq z$ existe un par de polinomios único $q(x), r(x)$ donde $r(x)$ es o bien el polinomio cero o de un grado menos que $\beta(x)$, tales que

$$\alpha(x) = q(x) \cdot \beta(x) + r(x)$$

Para demostración, véase Problema 4.

Si $r(x)$ es el polinomio cero, $\beta(x)$ se dice *divisor* de $\alpha(x)$ y se escribe $\beta(x) \mid \alpha(x)$.

Teorema del resto. Si $\alpha(x), x - b \in \mathscr{F}[x]$, el resto de dividir $\alpha(x)$ por $x - b$ es $\alpha(b)$.

Teorema del factor. Si $\alpha(x) \in \mathscr{F}[x]$ y $b \in \mathscr{F}$, $x - b$ es un *factor* de $\alpha(x)$ si, y solo si, $\alpha(\beta) = z$, es decir, $x - b$ es factor de $\alpha(x)$ si, y solo si, b es un cero de $\alpha(x)$.

De aquí se sigue

Teorema VI. Sea $\alpha(x) \in \mathscr{F}[x]$ de grado $m > 0$ y coeficiente dominante a. Si los elementos distintos $b_1, b_2, \ldots, b_m$ de $\mathscr{F}$ son ceros de $\alpha(x)$, entonces

$$\alpha(x) = a(x - b_1)(x - b_2) \ldots (x - b_m)$$

Para una demostración, véase Problema 5.

Teorema VII. Todo polinomio $\alpha(x) \in \mathscr{F}[x]$ de grado $m > 0$ tiene a lo más m ceros distintos en

Ejemplo 4:

(*a*) El polinomio $2x^2 + 7x - 15 \in Q[x]$ tiene los ceros $3/2, -5, \in Q$.

(*b*) El polinomio $x^2 + 2x + 3 \in C[x]$ tiene los ceros $-1 + \sqrt{2}\,i$ y $-1 - \sqrt{2}\,i$ en C, pero $x^2 + 2x + 3 \in Q[x]$ carece de ceros en Q.

Teorema VIII. Sean $\alpha(x), \beta(x) \in \mathscr{F}[x]$ tales que $\alpha(s) = \beta(s)$ para todo $s \in \mathscr{F}$. Entonces, si el número de elementos de $\mathscr{F}$ supera los grados de $\alpha(x)$ y $\beta(x)$, se tiene necesariamente $\alpha(x) = \beta(x)$.

Para una demostración, véase Problema 6.

Ejemplo 5: Se ve ahora claro que los polinomios del Ejemplo 1 son *distintos*, ya se consideren como funciones o como formas, pues el número de elementos de $\mathscr{F} = Z/(5)$ no supera al grado de ambos polinomios. Lo que en el Ejemplo 1 parecía entonces ser una contradicción con lo que el lector ya sabía, era debido naturalmente a que solo se tenía experiencia con cuerpos infinitos.

POLINOMIOS PRIMOS

No es difícil demostrar que las únicas unidades de un dominio polinómico $\mathscr{F}[x]$ son los elementos no nulos (es decir, los inversibles) del anillo de coeficientes $\mathscr{F}$. Así, pues, los únicos asociados de $\alpha(x) \in \mathscr{F}[x]$ son los elementos $v \cdot \alpha(x)$ de $\mathscr{F}[x]$ en que v es elemento inversible de $\mathscr{F}$.

Como para todo $v \neq z \in \mathscr{F}$ y todo $\alpha(x) \in \mathscr{F}[x]$,

$$\alpha(x) = (v^{-1} \cdot \alpha(x)) \cdot v$$

mientras que si $\alpha(x) = q(x) \cdot \beta(x)$

$$\alpha(x) = [v^{-1}\, q(x)] \cdot [v \cdot \beta(x)]$$

se deduce que (*a*) todo elemento inversible de $\mathscr{F}$ y todo asociado de $\alpha(x)$ es divisor de $\alpha(x)$ y (*b*) si $\beta(x) \mid \alpha(x)$ lo mismo se verifica con todo asociado de $\beta(x)$. Los elementos inversibles de $\mathscr{F}$ y los asociados de $\alpha(x)$ se llaman *divisores triviales* de $\alpha(x)$. Otros divisores de $\alpha(x)$, si los hay, se dicen *divisores no triviales*.

Un polinomio $\alpha(x) \in \mathscr{F}[x]$ de grado $m \geq 1$ se dice *polinomio primo* (*irreducible*) sobre $\mathscr{F}$ si solo tiene divisores triviales.

Ejemplo 6: (*a*) El polinomio $3x^2 + 2x + 1 \in R[x]$ es un polinomio primo sobre R.

(*b*) Todo polinomio $ax + b \in \mathscr{F}[x]$ con $a \neq z$, es primo sobre $\mathscr{F}$.

EL DOMINIO DE POLINOMIOS $C[x]$

Sea un polinomio

$$\beta(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in C[x]$$

de grado $m \geq 1$. En esta sección nos referiremos a ciertos teoremas elementales acerca de los ceros de tales polinomios y en particular acerca del subconjunto de todos los polinomios de $C[x]$ cuyos coeficientes son racionales. La mayoria de los teoremas se encuentran en cualquier texto de álgebra, si bien enunciado en términos de raíces de ecuaciones en vez de ceros de polinomios.

Supóngase que $r \in C$ es un cero de $\beta(x)$. Entonces, $\beta(r) = 0$ y como $b_m^{-1} \in C$, también $b_m^{-1} \cdot \beta(r) = 0$. Así que los ceros de $\beta(x)$ son precisamente los de su asociado mónico

$$\alpha(x) = b_m^{-1} \cdot \beta(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{m-1}x^{m-1} + x^m$$

Siempre que sea más cómodo trataremos de polinomios mónicos.

Es bien sabido que si $m = 1$, $\alpha(x) = a_0 + x$ tiene $-a_0$ como cero y si $m = 2$, $\alpha(x) = a_0 + a_1x + x^2$ tiene $\frac{1}{2}(-a_1 - \sqrt{a_1^2 - 4a_0})$ y $\frac{1}{2}(-a_1 + \sqrt{a_1^2 - 4a_0})$ como ceros. En el Capitulo 8 se vio cómo se hallan las n raices de cualquier $a \in C$; así que todo polinomio $x^n - a \in C[x]$ tiene al menos n ceros en C. Hay fórmulas (veánse Problemas 16-19) que dan los ceros de polinomios de grados 3 y 4. Pero se sabe también que no se pueden establecer fórmulas semejantes para cualesquiera polinomios de grado $m \geq 5$.

Por el Teorema VII, ningún polinomio $\alpha(x)$ de grado $m \geq 1$ puede tener más de m ceros distintos. En el párrafo anterior, $\alpha(x) = a_0 + a_1x + x^2$ tendrá dos ceros distintos si, y solo si, su discriminante $a_1^2 - 4a_0 \neq 0$. Diremos entonces que cada uno es un *cero simple* de $\alpha(x)$. No obstante, si $a_1^2 - 4a_0 = 0$, cada fórmula da $-\frac{1}{2}a_1$ como cero y entonces diremos que $-\frac{1}{2}a_1$ es un cero de *multiplicidad dos* de $\alpha(x)$ y enumeraremos los ceros así: $-\frac{1}{2}a_1$, $-\frac{1}{2}a_1$.

Ejemplo 7: (*a*) El polinomio $x^3 + x^2 - 5x + 3 = (x - 1)^2(x + 3)$ tiene -3 como cero simple y 1 como cero de multiplicidad 2.

(*b*) El polinomio $x^4 - x^3 - 3x^2 + 5x - 2 = (x - 1)^3(x + 2)$ tiene el cero simple -2 y el cero de multiplicidad tres, 1.

Aquí se supondrá como postulado el llamado

Teorema fundamental del álgebra. Todo polinomio $\alpha(x) \in C[x]$ de grado $m \geq 1$ tiene por lo menos un cero en C.

De aquí se sigue por inducción

Teorema IX. Todo polinomio $\alpha(x) \in C[x]$ de grado $m \geq 1$ tiene precisamente m ceros en C, contando por n ceros todo cero de multiplicidad n.

Y, por tanto,

Teorema X. Todo $\alpha(x) \in C[x]$ de grado $m \geq 1$ o bien es de primer grado o puede escribirse como producto de polinomios de primer grado.

Exceptuados los casos especiales arriba anotados, el problema de hallar los ceros de un polinomio dado es difícil y de él no se tratará aquí. En lo que queda de esta sección nos limitaremos a ciertos subconjuntos de $C[x]$ obtenidos por restricción del anillo de coeficientes.

En primer lugar, supongamos que

$$\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in R[x]$$

de grado $m \geq 1$ tiene el cero $r = a + bi$, o sea, que

$$\alpha(r) = a_0 + a_1r + a_2r^2 + \cdots + a_mr^m = s + ti = 0$$

Por el Problema 2, Capítulo 8, página 79, tenemos que

$$\alpha(\bar{r}) = a_0 + a_1\bar{r} + a_2\bar{r}^2 + \cdots + a_m\bar{r}^m = \overline{s + ti} = 0$$

de modo que

Teorema XI. Si $r \in C$ es un cero de un polinomio $\alpha(x)$ con coeficientes reales, $\bar{r}$ también es un cero de $\alpha(x)$.

Sea $r = a + bi$ con $b \neq 0$ un cero de $\alpha(x)$. Por el Teorema XI $\bar{r} = a - bi$ también es un cero y podemos escribir

$$\begin{aligned}\alpha(x) &= [x - (a + bi)][x - (a - bi)] \cdot \alpha_1(x) \\ &= [x^2 - 2ax + a^2 + b^2] \cdot \alpha_1(x)\end{aligned}$$

donde $\alpha_1(x)$ es un polinomio de grado inferior en dos al de $\alpha(x)$ y tiene coeficientes reales. Como un polinomio cuadrático con coeficientes reales tiene ceros imaginarios si, y solo si, su discriminante es negativo, tenemos

Teorema XII. Los polinomios de primer grado y los polinomios de segundo grado con discriminante negativo son los únicos polinomios $\in \mathscr{R}[x]$ que son primos de $\mathscr{R}$.

Teorema XIII. Un polinomio de grado impar $\in \mathscr{R}[x]$ tiene necesariamente un cero real.

Supóngase ahora que

$$\beta(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m \in Q[x]$$

Sea c el máximo común divisor de los numeradores de los b y d el mínimo común múltiplo de los denominadores de los b; entonces,

$$\alpha(x) = \frac{d}{c} \cdot \beta(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in Q[x]$$

tiene coeficientes enteros cuyos únicos divisores comunes son ± 1, los elementos inversibles de Z. Además, $\beta(x)$ y $\alpha(x)$ tienen precisamente los mismos ceros.

Si $r \in Q$ es un cero de $\alpha(x)$, es decir, si

$$\alpha(r) = a_0 + a_1r + a_2r^2 + \cdots + a_mr^m = 0$$

se sigue de inmediato que

(i) si $r \in Z$, entonces $r \mid a_0$

(ii) si $r = s/t$, fraccionario irreducible, entonces,

$$t^m \cdot \alpha(s/t) = a_0t^m + a_1st^{m-1} + a_2s^2t^{m-2} + \cdots + a_{m-1}s^{m-1}t + a_ms^m = 0$$

de modo que $s \mid a_0$ y $t \mid a_m$. Hemos demostrado el

Teorema XIV. Sea $\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$

un polinomio de grado $m \geq 1$ con coeficientes enteros. Si $s/t \in Q$, con $(s, t) = 1$, es un cero de $\alpha(x)$, entonces $s \mid a_0$ y $t \mid a_m$.

Ejemplo 8: (*a*) Los ceros racionales posibles de

$$\alpha(x) = 3x^3 + 2x^2 - 7x + 2$$

son ± 1, ± 2, $\pm\frac{1}{3}$, $\pm\frac{2}{3}$. Como $\alpha(1) = 0$, $\alpha(-1) \neq 0$, $\alpha(2) \neq 0$, $\alpha(-2) = 0$, $\alpha(\frac{1}{3}) = 0$, $\alpha(-\frac{1}{3}) \neq 0$, $\alpha(\frac{2}{3}) \neq 0$, $\alpha(-\frac{2}{3}) \neq 0$ los ceros racionales son, pues, 1, -2, $\frac{1}{3}$ y es, entonces, $\alpha(x) = 3(x-1)(x+2)(x-\frac{1}{3})$.

Nota. Por el Teorema VII, $\alpha(x)$ no puede tener más de tres ceros distintos. Así que una vez hallados éstos se pueden descartar todas las otras posibilidades no ensayadas. Aquí no era necesario ensayar las posibilidades $-\frac{1}{3}, \frac{2}{3}, -\frac{2}{3}$.

(*b*) Los ceros racionales posibles de

$$\alpha(x) = 4x^5 - 4x^4 - 5x^3 + 5x^2 + x - 1$$

son ± 1, $\pm\frac{1}{2}$, $\pm\frac{1}{4}$. Como $\alpha(1) = 0$, $\alpha(-1) = 0$, $\alpha(\frac{1}{2}) = 0$, $\alpha(-\frac{1}{2}) = 0$, se tiene

$$\alpha(x) = 4(x-1)(x+1)(x-\tfrac{1}{2})(x+\tfrac{1}{2})\cdot(x-1)$$

y los ceros racionales son 1, 1, -1, $\frac{1}{2}$, $-\frac{1}{2}$.

(*c*) Los ceros racionales posibles de

$$\alpha(x) = x^4 - 2x^3 - 5x^2 + 4x + 6$$

son ± 1, ± 2, ± 3, ± 6. Para éstos, solo $\alpha(-1) = 0$ y $\alpha(3) = 0$, así que

$$\alpha(x) = (x+1)(x-3)(x^2-2)$$

Como ninguno de los posibles ceros ± 1, ± 2 de $x^2 - 2$ es cero, resulta que $x^2 - 2$ es un polinomio primo sobre Q y los únicos ceros racionales de $\alpha(x)$ son $-1, 3$.

(*d*) De los posibles ceros racionales: $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{6}$, de $\alpha(x) = 6x^4 - 5x^3 + 7x^2 - 5x + 1$ solamente $\frac{1}{2}$ y $\frac{1}{3}$ son ceros. Así que $\alpha(x) = 6(x-\frac{1}{2})(x-\frac{1}{3})(x^2+1)$ con lo que $x^2 + 1$ es un polinomio primo sobre Q y los ceros racionales de $\alpha(x)$ son $\frac{1}{2}$, $\frac{1}{3}$.

(*e*) Los posibles ceros racionales de

$$\alpha(x) = 3x^4 - 6x^3 + 4x^2 - 10x + 2$$

son ± 1, ± 2, $\pm\frac{1}{3}$, $\pm\frac{2}{3}$. Pero como ninguno anula a $\alpha(x)$, éste es un polinomio primo sobre Q.

MAXIMO COMUN DIVISOR

Sean $\alpha(x)$ y $\beta(x)$ polinomios no nulos de $\mathscr{F}[x]$. El polinomio $d(x) \in \mathscr{F}[x]$ con las propiedades

(1) $d(x)$ es mónico,
(2) $d(x) \mid \alpha(x)$ y $d(x) \mid \beta(x)$,
(3) para todo $c(x) \in \mathscr{F}[x]$ tal que $c(x) \mid \alpha(x)$ y $c(x) \mid \beta(x)$ se tiene $c(x) \mid d(x)$, se llama máximo común divisor de $\alpha(x)$ y $\beta(x)$.

Es evidente (véase Problema 7) que el máximo común divisor de dos polinomios de $\mathscr{F}[x]$ puede hallarse de la misma manera que el máximo común divisor de dos enteros expuesta en el Capítulo 5. Con el objeto de variar, demostramos en el Problema 8

Teorema XV. Sean los polinomios no nulos $\alpha(x)$ y $\beta(x)$ de $\mathscr{F}[x]$. El polinomio mónico

(*b*) $\qquad d(x) = s(x)\cdot\alpha(x) + t(x)\cdot\beta(x), \quad s(x),\ t(x) \in \mathscr{F}[x]$

de mínimo grado es el máximo común divisor de $\alpha(x)$ y $\beta(x)$

Se deduce que

Teorema XVI. Sean $\alpha(x)$ de grado $m \geq 2$ y $\beta(x)$ de grado $n \geq 2$ de $\mathscr{F}[x]$. Hay polinomios no nulos $\mu(x)$ de grado $n-1$ a lo más y $\nu(x)$ de grado $m-1$ a lo más, de $\mathscr{F}[x]$ tales que

(*c*) $\qquad \mu(x)\cdot\alpha(x) + \nu(x)\cdot\beta(x) = z$

si, y solamente si, $\alpha(x)$ y $\beta(x)$ no son primos entre sí.

Para una demostración, véase Problema 9.

y

Teorema XVII. Si $\alpha(x)$, $\beta(x)$, $p(x) \in \mathscr{F}[x]$ con $\alpha(x)$ y $p(x)$ primos entre si, entonces $p(x) \mid \alpha(x) \cdot \beta(x)$ implica $p(x) \mid \beta(x)$.

En el Problema 10 se demuestra el

Teorema de factorización única. Todo polinomio $\alpha(x)$ de grado $m \geq 1$ y de coeficiente dominante a, de $\mathscr{F}[x]$, puede escribirse

$$\alpha(x) = a \cdot [p_1(x)]^{m_1} \cdot [p_2(x)]^{m_2} \cdots [p_t(x)]^{m_t}$$

donde los $p_i(x)$ son polinomios primos mónicos sobre $\mathscr{F}$ y los m_i son enteros positivos. Además, salvo el orden de los factores, la factorización es única.

Ejemplo 9: Descompóngase $\alpha(x) = 4x^4 + 3x^3 + 4x^2 + 4x + 6$ sobre $Z/(7)$ en un producto de polinomios primos.

Tenemos, sobrentendiendo que todos los coeficientes son clases residuales módulo 7,

$$\begin{aligned} \alpha(x) &= 4x^4 + 3x^3 + 4x^2 + 4x + 6 = 4x^4 + 24x^3 + 4x^2 + 4x + 20 \\ &= 4(x^4 + 6x^3 + x^2 + x + 5) = 4(x+1)(x^3 + 5x^2 + 3x + 5) \\ &= 4(x+1)(x+3)(x^2 + 2x + 4) = 4(x+1)(x+3)(x+3)(x+6) \\ &= 4(x+1)(x+3)^2(x+6) \end{aligned}$$

PROPIEDADES DEL DOMINIO DE POLINOMIOS $\mathscr{F}[x]$

El anillo de polinomios $\mathscr{F}[x]$ sobre un cuerpo $\mathscr{F}$ tiene ciertas propiedades que se corresponden con las del anillo Z de los enteros. Por ejemplo, ambos tienen elementos primos, ambos son anillos euclidianos (véase Problema 11) y ambos son anillos ideales principales (véase Teorema IX, Capítulo 10, página 108). Además, y de esto nos ocuparemos aquí principalmente, $\mathscr{F}[x]$ puede ser particionado por cualquier polinomio $\lambda(x) \in \mathscr{F}[x]$ de grado $n \geq 1$ en un anillo

$$\mathscr{F}[x]/(\lambda(x)) = \{[\alpha(x)], [\beta(x)], \ldots\}$$

de clases de equivalencia asi como Z lo es en el anillo $Z/(m)$. Para cualesquiera $\alpha(x)$, $\beta(x) \in \mathscr{F}[x]$ se define

(i) $$[\alpha(x)] = \{\alpha(x) + \mu(x) \cdot \lambda(x) : \mu(x) \in \mathscr{F}[x]\}$$

Entonces, $\alpha(x) \in [\alpha(x)]$, pues el elemento cero de $\mathscr{F}$ es también elemento de $\mathscr{F}[x]$, y $[\alpha(x)] = [\beta(x)]$ si, y solo si, $\alpha(x) \equiv \beta(x) \pmod{\lambda(x)}$, es decir, si, y solo si, $\lambda(x) \mid (\alpha(x) - \beta(x))$.

Definamos ahora la adición y la multiplicación entre estas clases de equivalencia por

$$[\alpha(x)] + [\beta(x)] = [\alpha(x) + \beta(x)]$$
$$[\alpha(x)] \cdot [\beta(x)] = [\alpha(x) \cdot \beta(x)]$$

y

respectivamente, dejando al lector la demostración

(*a*) La adición y la multiplicación son operaciones bien definidas sobre $\mathscr{F}[x]/(\lambda(x))$.

(*b*) $\mathscr{F}[x]/(\lambda(x))$ tiene $[z]$ como elemento cero y $[u]$ como unidad, donde z y u respectivamente son el cero y la unidad de $\mathscr{F}$.

(*c*) $\mathscr{F}[x]/(\lambda(x))$, es un anillo conmutativo unitario

En el Problema 12 demostramos el

Teorema XVIII. El anillo $\mathscr{F}[x]/(\lambda(x))$ contiene un subanillo isomorfo al cuerpo $\mathscr{F}$.

Si $\lambda(x)$ es de grado 1, es claro que $\mathscr{F}[x]/(\lambda(x))$ es el cuerpo $\mathscr{F}$; si $\lambda(x)$ es de grado 2, $\mathscr{F}[x]/(\lambda(x)$ consta de $\mathscr{F}$ junto con todas las clases de equivalencia $\{[a_0 + a_1 x] : a_0, a_1 \in \mathscr{F}, a_1 \neq z\}$; en general, si $\lambda(x)$ es de grado n, tenemos

$$\mathscr{F}[x]/(\lambda(x)) = \{[a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}] : a_i \in \mathscr{F}\}$$

Ahora bien, las definiciones de adición y multiplicación entre clases de equivalencia y el isomorfismo: $a_i \leftrightarrow [a_i]$ implican

$$\begin{aligned}[a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}] &= [a_0] + [a_1][x] + [a_2]\cdot[x]^2 + \cdots + [a_{n-1}]\cdot[x]^{n-1} \\ &= a_0 + a_1[x] + a_2[x]^2 + \cdots + a_{n-1}[x]^{n-1}\end{aligned}$$

Como una última simplificación, remplazando $[x]$ por ξ tenemos

$$\mathscr{F}[x]/(\lambda(x)) = \{a_0 + a_1\xi + a_2\xi^2 + \cdots + a_{n-1}\xi^{n-1} : a_i \in \mathscr{F}\}$$

En el Problema 13 se demuestra el

Teorema XIX. El anillo $\mathscr{F}[x]/(\lambda(x))$ es un cuerpo si, y solamente si, $\lambda(x)$ es un polinomio primo sobre $\mathscr{F}$.

Ejemplo 10: Considérese $\lambda(x) = x^2 - 3 \in Q[x]$ un polinomio primo sobre Q. De manera que

$$Q[x]/(x^2 - 3) = \{a_0 + a_1\xi : a_0, a_1 \in Q\}$$

es un cuerpo con respecto a la adición y multiplicación definidas como de ordinario excepto en que en la multiplicación hay que remplazar ξ^2 por 3. Es fácil hacer ver que la aplicación

$$a_0 + a_1\xi \leftrightarrow a_0 + a_1\sqrt{3}$$

es un isomorfismo de $Q[x]/(x^2 - 3)$ sobre

$$Q[\sqrt{3}] = \{a_0 + a_1\sqrt{3} : a_0, a_1 \in Q\},$$

el conjunto de todos los polinomios en $\sqrt{3}$ sobre Q. Evidentemente, $Q[\sqrt{3}] \subset R$ de modo que $Q[\sqrt{3}]$ es el mínimo cuerpo en que $x^2 - 3$ se factoriza enteramente.

El polinomio $x^2 - 3$ del Ejemplo 10 es el polinomio mónico sobre Q de grado mínimo que tiene $\sqrt{3}$ como raíz. Siendo único, se le llama el *polinomio mínimo de* $\sqrt{3}$ sobre Q. Nótese que el polinomio mínimo de $\sqrt{3}$ sobre R es $x - \sqrt{3}$.

Ejemplo 11: Sea $\mathscr{F} = Z/(3) = \{0, 1, 2\}$ y tómese $\lambda(x) = x^2 + 1$ un polinomio primo sobre $\mathscr{F}$. Constrúyase la tabla de adición y multiplicación para el cuerpo $\mathscr{F}[x]/(\lambda(x))$.

Aquí
$$\begin{aligned}\mathscr{F}[x]/(\lambda(x)) &= \{a_0 + a_1\xi : a_0, a_1 \in \mathscr{F}\} \\ &= \{0, 1, 2, \xi, 2\xi, 1 + \xi, 1 + 2\xi, 2 + \xi, 2 + 2\xi\}\end{aligned}$$

Como $\lambda(\xi) = \xi^2 + 1 = [0]$, tenemos $\xi^2 = [-1] = [2]$ ó 2. Las tablas son:

+	0	1	2	ξ	2ξ	$1+\xi$	$1+2\xi$	$2+\xi$	$2+2\xi$
0	0	1	2	ξ	2ξ	$1+\xi$	$1+2\xi$	$2+\xi$	$2+2\xi$
1	1	2	0	$1+\xi$	$1+2\xi$	$2+\xi$	$2+2\xi$	ξ	2ξ
2	2	0	1	$2+\xi$	$2+2\xi$	ξ	2ξ	$1+\xi$	$1+2\xi$
ξ	ξ	$1+\xi$	$2+\xi$	2ξ	0	$1+2\xi$	1	$2+2\xi$	2
2ξ	2ξ	$1+2\xi$	$2+2\xi$	0	ξ	1	$1+\xi$	2	$2+\xi$
$1+\xi$	$1+\xi$	$2+\xi$	ξ	$1+2\xi$	1	$2+2\xi$	2	2ξ	0
$1+2\xi$	$1+2\xi$	$2+2\xi$	2ξ	1	$1+\xi$	2	$2+\xi$	0	ξ
$2+\xi$	$2+\xi$	ξ	$1+\xi$	$2+2\xi$	2	2ξ	0	$1+2\xi$	1
$2+2\xi$	$2+2\xi$	2ξ	$1+2\xi$	2	$2+\xi$	0	ξ	1	$1+\xi$

Tabla 12-1

	0	1	2	ξ	2ξ	$1+\xi$	$1+2\xi$	$2+\xi$	$2+2\xi$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	ξ	2ξ	$1+\xi$	$1+2\xi$	$2+\xi$	$2+2\xi$
2	0	2	1	2ξ	ξ	$2+2\xi$	$2+\xi$	$1+2\xi$	$1+\xi$
ξ	0	ξ	2ξ	2	1	$2+\xi$	$1+\xi$	$2+2\xi$	$1+2\xi$
2ξ	0	2ξ	ξ	1	2	$1+2\xi$	$2+2\xi$	$1+\xi$	$2+\xi$
$1+\xi$	0	$1+\xi$	$2+2\xi$	$2+\xi$	$1+2\xi$	2ξ	2	1	ξ
$1+2\xi$	0	$1+2\xi$	$2+\xi$	$1+\xi$	$2+2\xi$	2	ξ	2ξ	1
$2+\xi$	0	$2+\xi$	$1+2\xi$	$2+2\xi$	$1+\xi$	1	2ξ	ξ	2
$2+2\xi$	0	$2+2\xi$	$1+\xi$	$1+2\xi$	$2+\xi$	ξ	1	2	2ξ

Tabla 12-2

Ejemplo 12: Sea $\mathscr{F} = Q$ y tómese $\lambda(x) = x^2 + x + 1$, un polinomio primo sobre $\mathscr{F}$. Hallar el simétrico multiplicativo de $\xi^2 + \xi + 1 \in \mathscr{F}[x]/(\lambda(x))$.

Aquí $\mathscr{F}[x]/(\lambda(x)) = \{a_0 + a_1\xi + a_2\xi^2 : a_0, a_1, a_2 \in Q\}$ y como $\lambda(\xi) = \xi^2 + \xi + 1 = 0$, tenemos $\xi^3 = -1 - \xi$ y $\xi^4 = -\xi - \xi^2$. Un procedimiento para hallar el simétrico pedido es:

hacer $(a_0 + a_1\xi + a_2\xi^2)(1 + \xi + \xi^2) = 1$,
multiplicar sustituyendo ξ^3 y ξ^4,
igualar los correspondientes coeficientes de ξ^0, ξ, ξ^2
y despejar a_0, a_1, a_2.

Por lo general, esto resulta más tedioso que seguir la demostración de existencia del simétrico en el Problema 13. Así, utilizando el algoritmo de la división, encontramos

$$1 = \tfrac{1}{3}(\xi^3 + \xi + 1)(1 - \xi) + \tfrac{1}{3}(\xi^2 + \xi + 1)(\xi^2 - 2\xi + 2)$$

Entonces, $$(\xi^3 + \xi + 1) \mid [1 - \tfrac{1}{3}(\xi^2 + \xi + 1)(\xi^2 - 2\xi + 2)]$$

de modo que $$\tfrac{1}{3}(\xi^2 + \xi + 1)(\xi^2 - 2\xi + 2) = 1$$

y así $\frac{1}{3}(\xi^2 - 2\xi + 2)$ es el simétrico pedido.

Ejemplo 13: Demostrar que el cuerpo $R[x]/(x^2 + 1)$ es isomorfo a C.

Tenemos $R[x]/(x^2 + 1) = \{a_0 + a_1\xi : a_0, a_1 \in R\}$. Como $\xi^2 = -1$, la aplicación

$$a_0 + a_1\xi \to a_0 + a_1 i$$

es un isomorfismo de $R[x]/(x^2 + 1)$ sobre C. Tenemos, pues, un segundo método para construir el cuerpo de los números complejos con el cuerpo de los números reales. No es posible, en cambio, utilizar tal procedimiento para construir el cuerpo de los números reales a partir de los racionales.

El Ejemplo 13 ilustra el

Teorema XX. Si $\alpha(x)$ de grado $m \geq 2$ es un elemento de $\mathscr{F}[x]$, existe un cuerpo $\mathscr{F}'$, con $\mathscr{F} \subset \mathscr{F}'$, en que $\alpha(x)$ tiene un cero.

Para una demostración, véase Problema 14.

Es de notar que sobre el cuerpo $\mathscr{F}'$ del Teorema XX, $\alpha(x)$ puede o no escribirse como producto de m factores de grado uno. Sin embargo, si $\alpha(x)$ no se factoriza completamente sobre $\mathscr{F}'$, tiene un factor primo de grado $n \geq 2$ que se puede utilizar para obtener un cuerpo $\mathscr{F}''$, con $\mathscr{F} \subset \mathscr{F}' \subset \mathscr{F}''$, en el cual $\alpha(x)$ tiene otro cero. Como $\alpha(x)$ tiene solamente un número finito de ceros, el procedimiento se puede reiterar siempre un número suficiente de veces para llegar así a un cuerpo $\mathscr{F}^{(i)}$ en que $\alpha(x)$ se factorice por completo.

Véase Problema 15.

Problemas resueltos

1. Demostrar: Sea $\mathscr{R}$ un anillo con unidad u; sea

$$\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in \mathscr{R}[x]$$

bien el polinomio nulo o bien de grado m; y sea

$$\beta(x) = b_0 + b_1x + b_2x^2 + \cdots + ux^n \in \mathscr{R}[x]$$

un polinomio mónico de grado n. Existe entonces un par de polinomios único $q_R(x)$, $r_R(x) \in \mathscr{R}[x]$ con $r_R(x)$ ya nulo, ya de grado $< n$ tal que

$$\text{(i)} \qquad \alpha(x) = q_R(x)\cdot\beta(x) + r_R(x)$$

Si $\alpha(x)$ es el polinomio nulo o si $n > m$, entonces (i) es válida con $q_R(x) = z$ y $r_R(x) = \alpha(x)$.

Sea $n \leq m$. El teorema es trivial una vez más si $m = 0$ o si $m = 1$ y $n = 0$. Para el caso $m = n = 1$, tómese $\alpha(x) = a_0 + a_1x$ y $\beta(x) = b_0 + ux$. Entonces,

$$\alpha(x) = a_0 + a_1x = a_1(b_0 + ux) + (a_0 - a_1b_0)$$

y el teorema es cierto con $q_R(x) = a_1$ y $r_R(x) = a_0 - a_1b_0$.

Vamos a emplear ahora el principio de inducción del Problema 27, Capítulo 3, página 37. Para ello supongamos que el teorema es cierto para todo $\alpha(x)$ de grado $\leq m - 1$ y consideremos $\alpha(x)$ de grado m. Ahora bien, $\gamma(x) = \alpha(x) - a_mx^{n-m}\cdot\beta(x) \in \mathscr{R}[x]$ y tiene grado $< m$. Por hipótesis,

$$\gamma(x) = \delta(x)\cdot\beta(x) + r(x)$$

con $r(x)$ de grado $n - 1$ a lo sumo. Entonces,

$$\alpha(x) = \gamma(x) + a_mx^{n-m}\cdot\beta(x) = \big(\delta(x) + a_mx^{n-m}\big)\cdot\beta(x) + r(x)$$
$$= q_R(x)\cdot\beta(x) + r_R(x)$$

donde $q_R(x) = \delta(x) + a_mx^{n-m}$ y $r_R(x) = r(x)$, como se requería.

Para demostrar la unicidad, supongamos

$$\alpha(x) = q_R(x)\cdot\beta(x) + r_R(x) = q'_R(x)\cdot\beta(x) + r'_R(x)$$

Entonces,

$$\big(q_R(x) - q'_R(x)\big)\cdot\beta(x) = r'_R(x) - r_R(x)$$

Pero $r'_R(x) - r_R(x)$ tiene un grado que es $n - 1$ a lo más, mientras que, al menos que $q_R(x) - q'_R(x) = z$, $(q_R(x) - q'_R(x))\cdot\beta(x)$ tiene grado n por lo menos. Así que $q_R(x) - q'_R(x) = z$ y entonces $r'_R(x) - r_R(x) = z$, lo cual demuestra la unicidad.

2. Demostrar: El resto a la derecha de dividir $\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m \in \mathscr{R}[x]$ por $x - b$, $b \in \mathscr{R}$, es $r_R = a_0 + a_1b + a_2b^2 + \cdots + a_mb^m$.

Considérese

$$\alpha(x) - r_R = a_1(x - b) + a_2(x^2 - b^2) + \cdots + a_m(x^m - b^m)$$
$$= \{a_1 + a_2(x + b) + \cdots + a_m(x^{m-1} + bx^{m-2} + \cdots + b^{m-1})\}\cdot(x - b)$$
$$= q_R(x)\cdot(x - b)$$

Entonces,

$$\alpha(x) = q_R(x)\cdot(x - b) + r_R$$

Según el Problema 1, el resto a la derecha es único; luego r_R es el resto a la derecha requerido.

3. En el anillo de polinomios $S[x]$ sobre S, el anillo del Ejemplo 1(*d*), Capítulo 11, página 114,

(*a*) Hallar el resto cuando $\alpha(x) = cx^4 + dx^3 + cx^2 + hx + g$ se divide por $\beta(x) = bx^2 + fx + d$.

(*b*) Comprobar que f es un cero de $\gamma(x) = cx^4 + dx^3 + cx^2 + bx + d$.

(*a*) Procederemos como en la división ordinaria con una variación. Como S es de característica dos, $s + (-t) = s + t$ para todo $s, t \in S$; luego, en el paso «cambiar los signos y sumar», sumaremos simplemente.

El resto es $r(x) = gx + f$.

$$
\begin{array}{r}
cx^2 + hx + b \\
\hline
bx^2 + fx + d \;\big)\; cx^4 + dx^3 + ex^2 + hx + g \\
cx^4 + ex^3 + fx^2 \\
\hline
hx^3 + hx^2 + hx \\
hx^3 + gx^2 + ex \\
\hline
bx^2 + dx + g \\
bx^2 + fx + d \\
\hline
ax + f
\end{array}
$$

(*b*) Aquí $f^2 = c$, $f^3 = cf = e$ y $f^4 = h$. Entonces

$$\begin{aligned} \gamma(f) &= ch + de + e^2 + bf + d \\ &= d + e + h + f + d = a \end{aligned}$$

como se pedía.

4. Demostrar el algoritmo de la división enunciado para el dominio de polinomios $\mathscr{F}[x]$.

Nota. Era necesario que $\beta(x)$ fuese mónico en el Teorema II, página 126, y en su nuevo enunciado para anillos conmutativos unitarios.

Supóngase ahora que $\alpha(x), \beta(x) \in \mathscr{F}[x]$ con $b_n \neq u$ por coeficiente dominante de $\beta(x)$. Entonces, como b_n^{-1} siempre existe en $\mathscr{F}$ y $\beta'(x) = b_n^{-1} \cdot \beta(x)$ es mónico, podemos escribir

$$\begin{aligned} \alpha(x) &= q'(x) \cdot \beta'(x) + r(x) \\ &= [b_n^{-1} q'(x)] \cdot [b_n \cdot \beta'(x)] + r(x) \\ &= q(x) \cdot \beta(x) + r(x) \end{aligned}$$

con $r(x)$ polinomio nulo o de grado inferior al de $\beta(x)$.

5. Demostrar: Sea $\alpha(x) \in \mathscr{F}[x]$ de grado $m > 0$ y coeficiente dominante a. Si los elementos distintos $b_1, b_2, \ldots, b_m$ de $\mathscr{F}$ son ceros de $\alpha(x)$, entonces $\alpha(x) = a(x - b_1)(x - b_2) \ldots (x - b_m)$.

Supóngase $m = 1$ de modo que $\alpha(x) = ax + a_1$ tenga como cero a b_1, por ejemplo. Entonces, $\alpha(b_1) = ab_1 + a_1 = z$, $a_1 = ab_1$ y

$$\alpha(x) = ax + a_1 = ax - ab_1 = a(x - b_1)$$

El teorema es cierto para $m = 1$.

Supóngase ahora que el teorema es cierto para $m = k$ y considérese $\alpha(x)$ de grado $k + 1$ con ceros $b_1, b_2, \ldots, b_{k+1}$. Como b_1 es un cero de $\alpha(x)$, tenemos por el teorema de factorización

$$\alpha(x) = q(x) \cdot (x - b_1)$$

donde $q(x)$ es de grado k con coeficiente dominante a. Como $\alpha(b_j) = q(b_j) \cdot (b_j - b_1) = z$ para $j = 2, 3, \ldots, k + 1$ y como $b_j - b_1 \neq z$ para todo $j \neq 1$, se sigue que $b_2, b_3, \ldots, b_{k+1}$ son k ceros distintos de $q(x)$. Por hipótesis,

$$q(x) = a(x - b_2)(x - b_3) \cdots (x - b_{k+1})$$

Entonces,

$$\alpha(x) = a(x - b_1)(x - b_2) \cdots (x - b_{k+1})$$

y la demostración por inducción queda completada.

6. Demostrar: Sean $\alpha(x), \beta(x) \in \mathscr{F}[x]$ tales que $\alpha(s) = \beta(s)$ para todo $s \in \mathscr{F}$. Entonces, si el número de elementos de $\mathscr{F}$ excede del grado de $\alpha(x)$ y de $\beta(x)$, se tiene necesariamente $\alpha(x) = \beta(x)$.

Hagamos $\gamma(x) = \alpha(x) - \beta(x)$. Entonces, $\gamma(x)$ o es el polinomio nulo o es de grado p que con seguridad no supera al mayor de los grados de $\alpha(x)$ y $\beta(x)$. Por hipótesis, $\gamma(s) = \alpha(s) - \beta(s)$ para todo $s \in \mathscr{F}$. Entonces, $\gamma(x) = z$ (pues si no $\gamma(x)$ tendría más ceros que su grado, en contra del Teorema VII, página 128) y $\alpha(x) = \beta(x)$ como se afirma.

7. Hallar el máximo común divisor de $\alpha(x) = 6x^5 + 7x^4 - 5x^3 - 2x^2 - x + 1$ y $\beta(x) = 6x^4 - 5x^3 - 19x^2 - 13x - 5$ sobre Q y expresarlo en la forma

$$d(x) = s(x) \cdot \alpha(x) + t(x) \cdot \beta(x)$$

Procediendo como en el problema correspondiente con enteros, encontramos

$$\alpha(x) = (x+2) \cdot \beta(x) + (24x^3 + 49x^2 + 30x + 11) = q_1(x) \cdot \beta(x) + r_1(x)$$

$$\beta(x) = \frac{1}{32}(8x - 23) \cdot r_1(x) + \frac{93}{32}(3x^2 + 2x + 1) = q_2(x) \cdot r_1(x) + r_2(x)$$

$$r_1(x) = \frac{1}{93}(256x + 352) \cdot r_2(x)$$

Como $r_2(x)$ no es mónico, es un asociado del máximo común divisor buscado $d(x) = x^2 + \frac{2}{3}x + \frac{1}{3}$.

De modo que

$$\begin{aligned} r_2(x) &= \beta(x) - q_2(x) \cdot r_1(x) \\ &= \beta(x) - q_2(x) \cdot \alpha(x) + q_1(x) \cdot q_2(x) \cdot \beta(x) \\ &= -q_2(x) \cdot \alpha(x) + \big(1 + q_1(x) \cdot q_2(x)\big) \cdot \beta(x) \\ &= -\frac{1}{32}(8x - 23) \cdot \alpha(x) + \frac{1}{32}(8x^2 - 7x - 14) \cdot \beta(x) \end{aligned}$$

y así, entonces, $d(x) = \frac{32}{279} r_2(x) = -\frac{1}{279}(8x - 23) \cdot \alpha(x) + \frac{1}{279}(8x^2 - 7x - 14) \cdot \beta(x)$

8. Demostrar: Sean los polinomios no nulos $\alpha(x)$ y $\beta(x)$ de $\mathscr{F}[x]$. El polinomio mónico

$$d(x) = s_0(x) \cdot \alpha(x) + t_0(x) \cdot \beta(x), \qquad s_0(x),\ t_0(x) \in \mathscr{F}[x]$$

de grado mínimo es el máximo común divisor de $\alpha(x)$ y $\beta(x)$.

Considérese el conjunto

$$S = \{s(x) \cdot \alpha(x) + t(x) \cdot \beta(x);\ s(x),\ t(x) \in \mathscr{F}[x]\}$$

Es claro que éste es un subconjunto no vacío de $\mathscr{F}[x]$ y, por tanto, contiene un polinomio no nulo $\delta(x)$ de grado mínimo. Para todo $b(x) \in S$, tenemos, por el algoritmo de la división, $b(x) = q(x) \cdot \delta(x) + r(x)$ donde $r(x) \in S$ (demostrar esto) o bien es el polinomio nulo o bien tiene grado menor que el de $\delta(x)$. Entonces $r(x) = z$ y $b(x) = q(x) \cdot \delta(x)$ de modo que todo elemento de S es un múltiplo de $\delta(x)$. Así, pues, $\delta(x) \mid \alpha(x)$ y $\delta(x) \mid \beta(x)$. Además, como $\delta(x) = \bar{s}_0(x) \cdot \alpha(x) + \bar{t}_0(x) \cdot \beta(x)$, cualquier divisor común $c(x)$ de $\alpha(x)$ y $\beta(x)$ es divisor de $\delta(x)$. Pero si $\delta(x)$ es mónico, es el máximo común divisor $d(x)$ de $\alpha(x)$ y $\beta(x)$; y si no, existiría un elemento inversible v tal que $v \cdot \delta(x)$ es mónico y $d(x) = v \cdot \delta(x)$ es el máximo común divisor buscado.

9. Demostrar: Sean $\alpha(x)$ de grado $m \geq 2$ y $\beta(x)$ de grado $n \geq 2$ de $\mathscr{F}[x]$. Hay entonces polinomios no nulos $\mu(x)$ de grado $n - 1$ a lo más y $\nu(x)$ de grado $m - 1$ a lo más en $\mathscr{F}[x]$ tales que

$$(c) \qquad \mu(x) \cdot \alpha(x) + \nu(x) \cdot \beta(x) = z$$

si, y solo si, $\alpha(x)$ y $\beta(x)$ no son primos entre sí

Supóngase que $\delta(x)$ de grado $p \geq 1$ es el máximo común divisor de $\alpha(x)$ y $\beta(x)$ y escríbase

$$\alpha(x) = \alpha_0(x) \cdot \delta(x), \qquad \beta(x) = \beta_0(x) \cdot \delta(x)$$

Es claro que $\alpha_0(x)$ tiene grado $\leq m - 1$ y $\beta_0(x)$ tiene grado $\leq n - 1$. Además,

$$\beta_0(x) \cdot \alpha(x) = \beta_0(x) \cdot \alpha_0(x) \cdot \delta(x) = \alpha_0(x) \cdot [\beta_0(x) \cdot \delta(x)] = \alpha_0(x) \cdot \beta(x)$$

de modo que

$$\beta_0(x) \cdot \alpha(x) + [-\alpha_0(x) \cdot \beta(x)] = z$$

y se tiene (c) con $\mu(x) = \beta_0(x)$ y $\nu(x) = -\alpha_0(x)$.

Recíprocamente, supóngase que se verifica (c) con $\alpha(x)$ y $\beta(x)$ primos entre sí. Por el Teorema XV, página 131, tenemos

$$u = s(x)\cdot\alpha(x) + t(x)\cdot\beta(x) \qquad \text{para ciertos } s(x),\ t(x) \in \mathscr{F}[x]$$

Entonces,

$$\begin{aligned}\mu(x) &= \mu(x)\cdot s(x)\cdot\alpha(x) + \mu(x)\cdot t(x)\cdot\beta(x)\\ &= s(x)\,[-\nu(x)\cdot\beta(x)] + \mu(x)\cdot t(x)\cdot\beta(x)\\ &= \beta(x)\,[\mu(x)\cdot t(x) - \nu(x)\cdot s(x)]\end{aligned}$$

y $\beta(x) \mid \mu(x)$. Pero esto es imposible; luego (c) no se verifica si $\alpha(x)$ y $\beta(x)$ son primos entre sí.

10. Demostrar: El teorema de factorización única es válido en $\mathscr{F}[x]$.

Considérese un polinomio $\alpha(x) \in \mathscr{F}[x]$. Si $\alpha(x)$ es primo, el teorema es trivial. Si $\alpha(x)$ es reducible, escribiendo $\alpha(x) = a\cdot\beta(x)\cdot\gamma(x)$ donde $\beta(x)$ y $\gamma(x)$ son polinomios mónicos de grado positivo menor que el de $\alpha(x)$, entonces o bien $\beta(x)$ y $\gamma(x)$ son polinomios primos, como se exige en el teorema, o uno o ambos son reducibles y pueden escribirse como producto de dos polinomios mónicos. Si todos los factores son primos, se tiene el teorema; si no . . . . Este proceso no puede seguirse indefinidamente (por ejemplo, en el caso extremo obtendríamos $\alpha(x)$ como producto de m polinomios de primer grado). La demostración de unicidad se deja al lector, quien también puede usar el procedimiento de inducción del Problema 27, Capítulo 3, página 37, en la primera parte de la demostración.

11. Demostrar: El anillo de polinomios $\mathscr{F}[x]$ sobre el cuerpo $\mathscr{F}$ es un anillo euclidiano.

Para todo polinomio no nulo $\alpha(x) \in \mathscr{F}[x]$ defínase $\theta(\alpha) = m$ donde m es el grado de $\alpha(x)$. Si $\alpha(x), \beta(x) \in \mathscr{F}[x]$ tienen, respectivamente, grados m y n, se sigue que $\theta(\alpha) = m$, $\theta(\beta) = n$, $\theta(\alpha\cdot\beta) = m + n$ y, por consiguiente, $\theta(\alpha\cdot\beta) \geq \theta(\alpha)$. Pero ya se ha establecido el algoritmo de la división:

$$\alpha(x) = q(x)\cdot\beta(x) + r(x)$$

donde $r(x)$ o bien es z o de grado inferior al de $\beta(x)$. Así, pues, o bien $r(x) = z$ o bien $\theta(r) < \theta(\beta)$, como se afirma.

12. Demostrar: El anillo $\mathscr{F}[x]/(\lambda(x))$ contiene un subanillo isomorfo al cuerpo $\mathscr{F}$.

Sean a, b elementos distintos de $\mathscr{F}$; entonces, $[a]$, $[b]$ son elementos diferentes de $\mathscr{F}[x]/(\lambda(x))$ puesto que $[a] = [b]$ si, y solo si, $\lambda(x) \mid (a - b)$.

Entonces, la aplicación $a \to [a]$ es un isomorfismo de $\mathscr{F}$ sobre un subconjunto de $\mathscr{F}[x]/(\lambda(x))$, pues es biyectiva y se preservan las operaciones de adición y multiplicación. Se deja al lector el demostrar que este subconjunto es un subanillo de $\mathscr{F}(x)/(\lambda(x))$.

13. Demostrar: El anillo $\mathscr{F}[x]/(\lambda(x))$ es un cuerpo si, y solo si, $\lambda(x)$ es un polinomio primo sobre $\mathscr{F}$.

Supóngase que $\lambda(x)$ es un polinomio primo sobre $\mathscr{F}$. Entonces para todo $[\alpha(x)] \neq [z]$ de $\mathscr{F}[x]/(\lambda(x))$ tenemos por el Teorema XV, página 131,

$$u = \alpha(x)\cdot\beta(x) + \lambda(x)\cdot\gamma(x) \qquad \text{para ciertos } \beta(x), \gamma(x) \in \mathscr{F}[x]$$

Ahora bien, $\lambda(x) \mid u - \alpha(x)\cdot\beta(x)$ de modo que $[\alpha(x)]\cdot[\beta(x)] = [u]$. Luego, todo elemento no nulo $[\alpha(x)] \in \mathscr{F}[x]/(\lambda(x)$ tiene simétrico multiplicativo y $\mathscr{F}[x]/(\lambda(x))$ es un cuerpo.

Supóngase que $\lambda(x)$ de grado $m \geq 2$ no es polinomio primo sobre $\mathscr{F}$ o sea que $\lambda(x) = \mu(x)\cdot\nu(x)$ donde $\mu(x), \nu(x) \in \mathscr{F}[x]$ tienen grados positivos s y t tales que $s + t = m$. Entonces, $s < m$ de modo que $\lambda(x) \nmid \mu(x)$ y $[\mu(x)] \neq [z]$; análogamente, $[\nu(x)] \neq [z]$. Pero $[\mu(x)]\cdot[\nu(x)] = [\mu(x)\cdot\nu(x)] = [\lambda(x)] = [z]$. Así, pues, como $[\mu(x)], [\nu(x)] \in \mathscr{F}[x]/(\lambda(x))$, se sigue que $\mathscr{F}[x]/(\lambda(x))$ tienen divisores de cero y no es un cuerpo.

14. Demostrar: Si $\alpha(x)$ de grado $m \geq 2$ es un elemento de $\mathscr{F}[x]$, existe un cuerpo $\mathscr{F}'$ con $\mathscr{F} \subset \mathscr{F}'$ en que $\alpha(x)$ tiene un cero.

El teorema es trivial si $\alpha(x)$ tiene un cero en $\mathscr{F}$; supóngase que no es así. Entonces existe un polinomio primo mónico $\lambda(x) \in \mathscr{F}[x]$ de grado $n \geq 2$ tal que $\lambda(x) \mid \alpha(x)$. Como $\lambda(x)$ es primo sobre $\mathscr{F}$, defínase $\mathscr{F}' = \mathscr{F}[x]/(\lambda(x))$.

Ahora, por el Teorema XVIII, página 132, $\mathscr{F} \subset \mathscr{F}'$ de modo que $\alpha(x) \in \mathscr{F}'[x]$. Así que existe $\xi \in \mathscr{F}'$ tal que $\lambda(\xi) = [z]$. Con lo cual ξ es un cero de $\alpha(x)$ y $\mathscr{F}'$ es un cuerpo que cumple lo exigido por el teorema.

15. Hallar un cuerpo en el cual $x^3 - 3 \in Q[x]$ (*a*) tiene un factor, (*b*) se factoriza completamente.

Considérese el cuerpo $Q[x]/(x^3 - 3) = \{a_0 + a_1\xi + a_2\xi^2 : a_0, a_1, a_2 \in Q\}$

(*a*) El cuerpo así definido es isomorfo a

$$\mathscr{F}' = \{a_0 + a_1\sqrt[3]{3} + a_2\sqrt[3]{9} : a_0, a_1, a_2 \in Q\}$$

en el cual $x^3 - 3$ tiene un cero.

(*b*) Como los ceros de $x^3 - 3$ son $\sqrt[3]{3}$, $\sqrt[3]{3}\,\omega$, $\sqrt[3]{3}\,\omega^2$, es claro que $x^3 - 3$ se factoriza enteramente en $\mathscr{F}'' = \mathscr{F}'[\omega]$.

16. Derivar fórmulas para los ceros del polinomio cúbico $\alpha(x) = a_0 + a_1x + a_2x^2 + x^3$ sobre C si $a_0 \neq 0$.

La deducción se basa en dos cambios a nuevas variables:

(i) Si $a_2 = 0$, hágase $x = y$ y procédase como en (ii) abajo; si $a_2 \neq 0$, hágase $x = y + v$ y elíjase v de modo que la cúbica que resulte carezca del término en y^2. Como el coeficiente de este término es $a_2 + 3v$, la relación apropiada es $x = y - a_2/3$. Sea el polinomio resultante

$$\beta(y) = \alpha(y - a_2/3) = q + py + y^3$$

Si $q = 0$, los ceros de $\beta(y)$ son 0, $\sqrt{-p}$, $-\sqrt{-p}$ y los ceros de $\alpha(x)$ se obtienen disminuyendo cada cero de $\beta(y)$ en $a_2/3$. Si $q \neq 0$ pero $p = 0$, los ceros de $\beta(y)$ son las tres raíces cúbicas ρ, $\omega\rho$, $\omega^2\rho$ (véase Capítulo 8) de $-q$, de donde los ceros de $\alpha(x)$ se obtienen como antes. Para el caso $pq \neq 0$,

(ii) Hágase $y = z - p/3z$ para tener

$$\gamma(z) = \beta(z - p/3z) = z^3 + q - p^3/27z^3 = \frac{z^6 + qz^3 - p^3/27}{z^3}$$

Entonces, cualquier cero, s por ejemplo, del polinomio $\delta(z) = z^6 + qz^3 - p^3/27$ da el cero $s - p/3s - a_2/3$ de $\alpha(x)$; los seis ceros de $\delta(z)$ dan, como se puede demostrar, cada cero de $\alpha(x)$ dos veces. Escríbase

$$\delta(z) = [z^3 + \tfrac{1}{2}(q - \sqrt{q^2 + 4p^3/27})] \cdot [z^3 + \tfrac{1}{2}(q + \sqrt{q^2 + 4p^3/27})]$$

y denótense los ceros de $z^3 + \frac{1}{2}(q - \sqrt{q^2 + 4p^3/27})$ por $A, \omega A, \omega^2 A$. Los ceros de $\alpha(x)$ son entonces: $A - p/3A - a_2/3$, $\omega A - \omega^2 p/3A - a_2/3$, y $\omega^2 A - \omega p/3A - a_2/3$.

17. Hallar los ceros de $\alpha(x) = -11 - 3x + 3x^2 + x^3$.

La sustitución $x = y - 1$ da

$$\beta(y) = \alpha(y - 1) = -6 - 6y + y^3$$

A su vez, la sustitución $y = z + 2/z$ da

$$\gamma(z) = \beta(z + 2/z) = z^3 + 8/z^3 - 6 = \frac{z^6 - 6z^3 + 8}{z^3} = \frac{(z^3 - 2)(z^3 - 4)}{z^3}$$

Tómese $A = \sqrt[3]{2}$; entonces los ceros de $\alpha(x)$ son

$$\sqrt[3]{2} + \sqrt[3]{4} - 1, \quad \omega\sqrt[3]{2} + \omega^2\sqrt[3]{4} - 1, \quad \omega^2\sqrt[3]{2} + \omega\sqrt[3]{4} - 1$$

El lector demostrará ahora que, salvo el orden, estos ceros se obtienen tomando $A = \sqrt[3]{4}$.

18. Obtener un procedimiento para hallar los ceros del polinomio de cuarto grado

$$\alpha(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + x^4 \in C[x], \qquad \text{si } a_0 \neq 0.$$

Si $a_3 \neq 0$, hágase $x = y - a_3/4$ para obtener

$$\beta(y) = \alpha(y - a_3/4) = b_0 + b_1y + b_2y^2 + y^4$$

Ahora bien,
$$\begin{aligned}\beta(y) &= (p + 2qy + y^2)(r - 2qy + y^2)\\ &= pr + 2q(r-p)y + (r + p - 4q^2)y^2 + y^4\end{aligned}$$

siempre que existan $p, q, r \in C$ que verifiquen

$$pr = b_0, \quad 2q(r-p) = b_1, \quad r + p - 4q^2 = b_2$$

Si $b_1 = 0$, tómese $q = 0$; si no, con $q \neq 0$, se halla

$$2p = b_2 + 4q^2 - b_1/2q \qquad \text{y} \qquad 2r = b_2 + 4q^2 + b_1/2q$$

Como $2p \cdot 2r = 4b_0$, tenemos

$$\text{(i)} \qquad 64q^6 + 32b_2q^4 + 4(b_2^2 - 4b_0)q^2 - b_1^2 = 0$$

Así que considerando el primer miembro de (i) como un polinomio de tercer grado en q^2, cualquiera de sus ceros distinto de 0 dará la factorización pedida. Entonces, con los cuatro ceros de $\beta(y)$, los ceros de $\alpha(x)$ se obtienen disminuyendo cada uno de éstos en $a_3/4$.

19. Hallar los ceros de $\alpha(x) = 35 - 16x - 4x^3 + x^4$.

Con $\alpha = y + 1$, obtenemos

$$\beta(y) = \alpha(y+1) = 16 - 24y - 6y^2 + y^4$$

Aquí, (i) del Problema 18 se convierte en

$$64q^6 - 192q^4 - 112q^2 - 576 = 16(q^2 - 4)(4q^4 + 4q^2 + 9) = 0$$

Tómese $q = 2$; entonces $p = 8$ y $r = 2$ de manera que

$$16 - 24y - 6y^2 + y^4 = (8 + 4y + y^2)(2 - 4y + y^2)$$

con ceros $-2 \pm 2i$ y $2 \pm \sqrt{2}$. Los ceros de $\alpha(x)$ son $-1 \pm 2i$ y $3 \pm \sqrt{2}$.

Problemas propuestos

20. Dar un ejemplo de dos polinomios en x de grado 3 con coeficientes enteros y cuya suma sea de grado 2.

21. Hallar la suma y producto de cada par de polinomios sobre el anillo de coeficientes indicado. (Para comodidad, se han remplazado $[a], [b], \ldots,$ por $a, b, \ldots,$)

(a) $4 + x + 2x^2$, $1 + 2x + 3x^2$; $Z/(5)$

(b) $1 + 5x + 2x^2$, $7 + 2x + 3x^2 + 4x^3$; $Z/(8)$

(c) $2 + 2x + x^3$, $1 + x + x^2 + x^4$; $Z/(3)$

Resp. (a) $3x$; $4 + 4x + x^2 + 2x^3 + x^4$

(c) $x^2 + x^3 + x^4$; $2 + x + x^2 + x^7$

22. En el anillo de polinomios $S[x]$ sobre S, el anillo del Problema 2, Capítulo 10, página 108, comprobar:

(*a*) $(b + gx + fx^2) + (d + gx) = c + ex + fx^2$

(*b*) $(b + gx + fx^2)(d + cx) = b + ax + ex^2 + bx^3$

(*c*) $(b + gx + fx^2)(d + ex) = b + ex + bx^2$

(*d*) $f + bx$ y $e + ex$ son divisores de cero

(*e*) c es un cero de $f + cx + fx^2 + ex^3 + dx^4$.

23. Dados $\alpha(x), \beta(x), \gamma(x) \in \mathscr{F}[x]$ con coeficientes dominantes respectivos a, b, c y supuesto $\alpha(x) = \beta(x) \cdot \gamma(x)$, demostrar que $\alpha(x) = a \cdot \beta'(x) \cdot \gamma'(x)$ con $\beta'(x)$ y $\gamma'(x)$ polinomios mónicos.

24. Demostrar que $\mathscr{D}[x]$ no es un cuerpo para cualquier dominio de integridad $\mathscr{D}$.
Sugerencia. Sea $\alpha(x) \in \mathscr{D}[x]$ de grado > 0 y supóngase que $\beta(x) \in \mathscr{D}[x]$ es un simétrico multiplicativo de $\alpha(x)$. Entonces $\alpha(x) \cdot \beta(x)$ tiene grado > 0, una contradicción.

25. Factorizar en productos de polinomios primos sobre (i) Q, (ii) R, (iii) C.

(*a*) $x^4 - 1$ (*c*) $6x^4 + 5x^3 + 4x^2 - 2x - 1$

(*b*) $x^4 - 4x^2 - x + 2$ (*d*) $4x^5 + 4x^4 - 13x^3 - 11x^2 + 10x + 6$

Resp. (*a*) $(x - 1)(x + 1)(x^2 + 1)$ sobre Q, R; $(x - 1)(x + 1)(x - i)(x + i)$ sobre C

(*d*) $(x - 1)(2x + 1)(2x + 3)(x^2 - 2)$ sobre Q; $(x - 1)(2x + 1)(2x + 3)(x - \sqrt{2})(x + \sqrt{2})$ sobre R, C

26. Factorizar en productos de polinomios primos sobre el cuerpo indicado. (Véase nota al Problema 21.)

(*a*) $x^2 + 1$; $Z/(5)$ (*c*) $2x^2 + 2x + 1$; $Z/(5)$

(*b*) $x^2 + x + 1$; $Z/(3)$ (*d*) $3x^3 + 4x^2 + 3$; $Z/(5)$

Resp. (*a*) $(x + 2)(x + 3)$, (*d*) $(x + 2)^2(3x + 2)$

27. Factorizar $x^4 - 1$ sobre (*a*) $Z/(11)$, (*b*) $Z/(13)$.

28. En (*d*) del Problema 26 obtener también $3x^3 + 4x^2 + 3 = (x + 2)(x + 4)(3x + 1)$. Explicar por qué esto no contradice al teorema de factorización única.

29. En el anillo de polinomios $S[x]$ sobre S, el anillo del Ejemplo 1(*d*), Capítulo 11, página 114,

(*a*) Demostrar que $bx^2 + ex + g$ y $gx^2 + dx + b$ son polinomios primos.

(*b*) Factorizar $hx^4 + ex^3 + cx^2 + b$.

Resp. (*b*) $(bx + b)(cx + g)(gx + d)(hx + e)$.

30. Hallar todos los ceros sobre C de los polinomios del Problema 25.

31. Hallar todos los ceros de los polinomios del Problema 26. *Resp.* (*a*) 2, 3; (*d*) 1, 3, 3

32. Hallar todos los ceros del polinomio del Problema 29(*b*). *Resp.* b, e, f, d

33. Enumerar los polinomios de la forma $3x^2 + cx + 4$ que son primos sobre $Z/(5)$.
Resp. $3x^2 + 4$, $3x^2 + x + 4$, $3x^2 + 4x + 4$

34. Enumerar todos los polinomios de grado 4 primos sobre $Z/(2)$.

35. Demostrar los Teoremas VII, IX y XIII.

36. Demostrar: Si $a + b\sqrt{c}$ con $a, b, c \in Q$ y si no siendo C un cuadrado perfecto es un cero de $\alpha(x) \in Z[x]$, también lo es $a - b\sqrt{c}$.

37. Sea $\mathscr{R}$ un anillo conmutativo unitario. Demostrar que $\mathscr{R}[x]$ es un anillo ideal principal. ¿Cuáles son los ideales primos?

38. Formar polinomios $\alpha(x) \in Z[x]$ de mínimo grado que tengan entre sus ceros:

(*a*) $\sqrt{3}$ y 2 (*c*) 1 y $2 + 3\sqrt{5}$ (*e*) $1 + i$ de multiplicidad 2

(*b*) i y 3 (*d*) $-1 + i$ y $2 - 3i$

Resp. (*a*) $x^3 - 2x^2 - 3x + 6$, (*d*) $x^4 - 2x^3 + 7x^2 + 18x + 26$

39. Verificar que el polinomio mínimo de $\sqrt{3} + 2i$ sobre $\mathscr{R}$ es de grado 2 y sobre Q es de grado 4.

40. Hallar el máximo común divisor de cada par $\alpha(x)$, $\beta(x)$ sobre el anillo de coeficientes indicado y expresarlo en la forma $s(x) \cdot \alpha(x) + t(x) \cdot \beta(x)$.

(*a*) $x^5 + x^4 - x^3 - 3x + 2$, $x^3 + 2x^2 - x - 2$; Q

(*b*) $3x^4 - 6x^3 + 12x^2 + 8x - 6$, $x^3 - 3x^2 + 6x - 3$; Q

(*c*) $x^5 - 3ix^3 - 2ix^2 - 6$, $x^2 - 2i$; C

(*d*) $x^5 + 3x^3 + x^2 + 2x + 2$, $x^4 + 3x^3 + 3x^2 + x + 2$; $Z/(5)$

(*e*) $x^5 + x^3 + x$, $x^4 + 2x^3 + 2x$; $Z(3)$

(*f*) $cx^4 + hx^3 + ax^2 + gx + e$, $gx^3 + hx^2 + dx + g$; S del Ejemplo 1(*d*), Capítulo 11, página 114

Resp. (*b*) $\frac{1}{447}(37x^2 - 108x + 177) \cdot \alpha(x) + \frac{1}{447}(-111x^3 + 213x^2 - 318x - 503) \cdot \beta(x)$

(*d*) $(x + 2) \cdot \alpha(x) + (4x^2 + x + 2) \cdot \beta(x)$

(*f*) $(gx + h) \cdot \alpha(x) + (cx^2 + hx + e) \cdot \beta(x)$

41. Demostrar el Teorema XVII, página 132.

42. Demostrar que todo polinomio de grado 2 de $\mathscr{F}[x]$ del Ejemplo 11, página 133, se descompone completamente en factores en $\mathscr{F}[x]/(x^2 + 1)$ dando los factores.

Respuesta parcial. $x^2 + 1 = (x + \xi)(x + 2\xi)$; $x^2 + x + 2 = (x + \xi + 2)(x + 2\xi + 2)$;
$2x^2 + x + 1 = (x + \xi + 1)(2x + \xi + 2)$

43. Estudiar el cuerpo $Q[x]/(x^3 - 3)$. (Véase Ejemplo 10, página 133.)

44. Hallar el simétrico multiplicativo de $\xi^2 + 2$ en (*a*) $Q[x]/(x^3 + x + 2)$, (*b*) $\mathscr{F}[x]/(x^2 + x + 1)$ si $\mathscr{F} = Z/(5)$.
Resp. (*a*) $\frac{1}{6}(1 - 2\xi - \xi^2)$, (*b*) $\frac{1}{3}(\xi + 2)$

Capítulo 13

Espacios vectoriales

INTRODUCCION

En este capítulo se define y estudia un tipo de sistema algebraico llamado espacio vectorial. Antes de hacer una definición formal, recordemos que en la física elemental hay que tratar con dos tipos de cantidades: (*a*) escalares (tiempo, temperatura, rapidez) que tienen magnitud solamente y (*b*) vectores (fuerza, velocidad, aceleración) que tienen magnitud y dirección, que se representan frecuentemente por flechas. Por ejemplo, considérese en la Fig. 13-1 un plano dado en el cual se ha establecido un sistema de coordenadas rectangulares y un vector $\xi_1 = OP = (a, b)$ que una el origen al punto $P(a, b)$. La magnitud de ξ_1 (longitud de OP) viene dada por $r = \sqrt{a^2 + b^2}$ y la dirección (el ángulo θ, siempre medido a partir del eje positivo x) la determina cualquiera de las relaciones sen $\theta = b/r$, cos $\theta = a/r$, tg $\theta = b/a$.

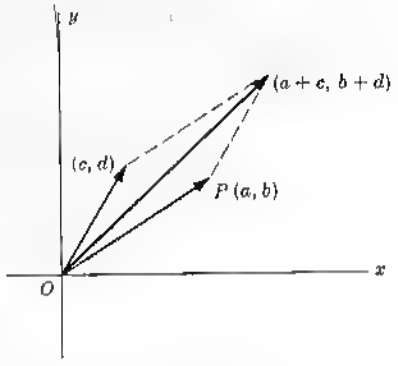


Fig. 13-1

Entre estos vectores se definen dos operaciones:

Multiplicación escalar. Sea el vector $\xi_1 = (a, b)$ que representa una fuerza aplicada en O. El producto del escalar 3 y el vector ξ_1 definido por $3\xi_1 = (3a, 3b)$ representa una fuerza aplicada en O que tiene el sentido de ξ_1 y tres veces su magnitud. Análogamente, $-2\xi_1$ representa una fuerza aplicada en O que tiene dos veces la magnitud de ξ_1, pero de sentido opuesto al de ξ_1.

Adición vectorial. Si $\xi_1 = (a, b)$ y $\xi_2 = (c, d)$ representan dos fuerzas aplicadas en O, su resultante ξ (la fuerza única aplicada en O que tiene el mismo efecto que las dos fuerzas ξ_1 y ξ_2) es dada por $\xi = \xi_1 + \xi_2 = (a + c, b + d)$ obtenida por la ley del paralelogramo.

En el ejemplo anterior es evidente que todo escalar $s \in R$ y todo vector $\xi \in R \times R$. No puede haber confusión al utilizar $(+)$ para denotar tanto la adición de vectores como la de escalares.

Denótese por V el conjunto de todos los vectores del plano (es decir, $V = R \times R$). Ya que V tiene un elemento neutro o cero $\zeta = (0, 0)$ y todo $\xi = (a, b) \in V$ tiene un simétrico aditivo u opuesto $-\xi = (-a, -b) \in V$ tal que $\xi + (-\xi) = \zeta$, V es un grupo aditivo abeliano. Además, para cualesquiera s, $t \in R$ y ξ, $\eta \in V$, se verifican las propiedades siguientes:

$$s(\xi + \eta) = s\xi + s\eta \qquad (s + t)\xi = s\xi + t\xi$$

$$s(t\xi) = (st)\xi \qquad 1\xi = \xi$$

Ejemplo 1: Considérense los vectores $\xi = (1, 2)$, $\eta = (\frac{1}{2}, 0)$, $\sigma = (0, -3/2)$. Entonces,

(*a*) $3\xi = 3(1, 2) = (3, 6)$, $2\eta = (1, 0)$, y $3\xi + 2\eta = (3, 6) + (1, 0) = (4, 6)$.

(*b*) $\xi + 2\eta = (2, 2)$, $\eta + \sigma = (\frac{1}{2}, -3/2)$, y $5(\xi + 2\eta) - 4(\eta + \sigma) = (8, 16)$.

ESPACIOS VECTORIALES

Sea $\mathscr{F}$ un cuerpo y V un grupo aditivo abeliano tales que existe una multiplicación escalar de V por $\mathscr{F}$ que asocia a todo $s \in \mathscr{F}$ y todo $\xi \in V$ el elemento $s\xi \in V$. Entonces, V se llama *espacio vectorial sobre* $\mathscr{F}$ si, siendo u la unidad de $\mathscr{F}$, se tiene,

$$\text{(i)}\quad s(\xi+\eta) = s\xi + s\eta \qquad \text{(iii)}\quad s(t\xi) = (st)\xi$$
$$\text{(ii)}\quad (s+t)\xi = s\xi + t\xi \qquad \text{(iv)}\quad u\xi = \xi$$

para cualesquiera $s, t \in \mathscr{F}$ y cualesquiera $\xi, \eta \in V$.

Es evidente que para llegar a la definición de espacio vectorial se ha utilizado como guia el conjunto de todos los vectores planos de la sección anterior. Pero, como se verá por los ejemplos que siguen, los elementos de un espacio vectorial, esto es los vectores, no son necesariamente cantidades que se puedan representar por flechas.

Ejemplo 2: (*a*) Sea $\mathscr{F} = R$ y $V = V_2(R) = \{(a_1, a_2): a_1, a_2 \in R\}$ con adición y multiplicación escalar definidas como en la primera sección. Entonces, claro está, V es un espacio vectorial sobre $\mathscr{F}$; en verdad, citamos el ejemplo para indicar una sencilla generalización: Sea $\mathscr{F} = R$ y $V = V_n(R) = \{(a_1, a_2, \ldots, a_n): a_i \in R\}$ con adición y multiplicación escalar definidas por

$$\begin{aligned}\xi + \eta &= (a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)\\ &= (a_1+b_1, a_2+b_2, \ldots, a_n+b_n), \qquad \xi, \eta \in V_n(R)\end{aligned}$$

y

$$s\xi = s(a_1, a_2, \ldots, a_n) = (sa_1, sa_2, \ldots, sa_n), \qquad s \in R,\ \xi \in V_n(R)$$

Entonces $V_n(R)$ es un espacio vectorial sobre R.

(*b*) Sea $\mathscr{F} = R$ y $V_n(C) = \{(a_1, a_2, \ldots, a_n): a_i \in C\}$ con adición y multiplicación escalar como en (*a*). $V_n(C)$ es un espacio vectorial sobre R.

(*c*) Sea $\mathscr{F}$ un cuerpo cualquiera, $V = \mathscr{F}[x]$ el dominio de polinomios en x sobre $\mathscr{F}$ y definase la adición y la multiplicación escalar como la adición y multiplicación ordinarias en $\mathscr{F}[x]$. Entonces V es un espacio vectorial sobre $\mathscr{F}$.

Sean $\mathscr{F}$ un cuerpo con elemento cero z y V un espacio vectorial sobre $\mathscr{F}$. Como V es un grupo aditivo abeliano, tiene un elemento cero único ζ y para cada elemento $\xi \in V$, existe un simétrico aditivo único $-\xi$ tal que $\xi + (-\xi) = \zeta$. Por las leyes distributivas (i) y (ii), encontramos para todo $s \in \mathscr{F}$ y $\xi \in V$,

$$s\xi + z\xi = (s+z)\xi = s\xi = s\xi + \zeta$$

y

$$s\xi + s\zeta = s(\xi+\zeta) = s\xi = s\xi + \zeta$$

Luego, $z\xi = \zeta$ y $s\zeta = \zeta$.

Enunciamos estas propiedades junto con otras que establecerá el lector, como

Teorema I. En un espacio vectorial V sobre $\mathscr{F}$ con z, el elemento cero de $\mathscr{F}$ y ζ el elemento cero de V, tenemos

(1) $s\zeta = \zeta$ para todo $s \in \mathscr{F}$
(2) $z\xi = \zeta$ para todo $\xi \in V$
(3) $(-s)\xi = s(-\xi) = -(s\xi)$ para todo $s \in \mathscr{F}$ y $\xi \in V$
(4) Si $s\xi = \zeta$, es $s = z$ o $\xi = \zeta$

SUBESPACIO DE UN ESPACIO VECTORIAL

Un subconjunto no vacio U de un espacio vectorial V sobre $\mathscr{F}$ es un *subespacio* de V si U es a su vez un espacio vectorial sobre $\mathscr{F}$ con respecto a las operaciones definidas sobre V. De aqui se sigue el

Teorema II. Un subconjunto no vacío U de un espacio vectorial V sobre $\mathscr{F}$ es un subespacio de V si, y solo si, U es cerrado con respecto a la multiplicación escalar y la adición vectorial definidas sobre V.

Para demostración, véase Problema 1.

Ejemplo 3: Considérese el espacio vectorial $V = V_3(R) = \{(a, b, c): a, b, c \in R\}$ sobre R. Por el Teorema II, el subconjunto $U = \{(a, b, 0): a, b \in R\}$ es un subespacio de V puesto que para todo $s \in R$ y $(a, b, 0), (c, d, 0) \in U$ tenemos

$$(a, b, 0) + (c, d, 0) = (a + c, b + d, 0) \in U$$

y

$$s(a, b, 0) = (sa, sb, 0) \in U$$

En el Ejemplo 3, V es el conjunto de los vectores del espacio ordinario en tanto que U es el conjunto de dichos vectores que están en el plano XOY. Análogamente, $W = \{(a, 0, 0): a \in R\}$ es el conjunto de los vectores sobre el eje X. Evidentemente, W es un subespacio tanto de U como de V.

Sea $\xi_1, \xi_2, \ldots, \xi_m \in V$ un espacio vectorial sobre $\mathscr{F}$. Se entiende por *combinación lineal* de estos m vectores el vector $\xi \in V$ dado por

$$\xi = \sum c_i\xi_i = c_1\xi_1 + c_2\xi_2 + \cdots + c_m\xi_m, \qquad c_i \in \mathscr{F}$$

Consideremos ahora dos de tales combinaciones lineales $\sum c_i\xi_i$ y $\sum d_i\xi_i$. Como

$$\sum c_i\xi_i + \sum d_i\xi_i = \sum (c_i + d_i)\xi_i$$

$$s \sum c_i\xi_i = \sum (sc_i)\xi_i$$

y, para todo $s \in \mathscr{F}$,
tenemos, por el Teorema II,

Teorema III. El conjunto U de todas las combinaciones lineales de un conjunto arbitrario S de vectores de un espacio (vectorial) V, es un subespacio de V.

El subespacio U de V definido en el Teorema III se dice *generado* por S. A su vez, los vectores de S se dicen *generadores* del espacio U.

Ejemplo 4: Considérese el espacio $V_3(R)$ del Ejemplo 3 y los subespacios

$$U = \{s(1, 2, 1) + t(3, 1, 5): s, t \in R\}$$

generado por $\xi_1 = (1, 2, 1)$ y $\xi_2 = (3, 1, 5)$

y

$$W = \{a(1, 2, 1) + b(3, 1, 5) + c(3, -4, 7): a, b, c \in R\}$$

generado por ξ_1, ξ_2 y $\xi_3 = (3, -4, 7)$

Decimos ahora que U y W son subespacios idénticos de V. Pues como $(3, -4, 7) = -3(1, 2, 1) + 2(3, 1, 5)$, podemos escribir

$$\begin{aligned} W &= \{(a - 3c)(1, 2, 1) + (b + 2c)(3, 1, 5): a, b, c \in R\} \\ &= \{s'(1, 2, 1) + t'(3, 1, 5): s', t' \in R\} \\ &= U \end{aligned}$$

Sea

$$U = \{k_1\xi_1 + k_2\xi_2 + \cdots + k_m\xi_m : k_i \in \mathscr{F}\}$$

el espacio generado por $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$, un subconjunto de vectores de V sobre $\mathscr{F}$. Como U contiene el vector cero $\zeta \in V$ (¿por qué?); entonces, si $\zeta \in S$ se le puede excluir de S, con lo que queda un subconjunto propio que también genera a U. Además, como lo indica el Ejemplo 4, si algún vector, ξ_j, por ejemplo, de S se puede escribir como combinación lineal de otros vectores de S, entonces ξ_j puede excluirse también de S y los vectores que quedan también generan a U. Lo cual plantea el problema sobre el mínimo número de vectores necesarios para generar un espacio dado U y la propiedad característica de un tal conjunto.

Véase también Problema 2.

DEPENDENCIA LINEAL

Un conjunto no vacio $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ de vectores de un espacio vectorial V sobre $\mathscr{F}$ se dice *linealmente dependiente* sobre $\mathscr{F}$ si, y sólo si, existen elementos $k_1, k_2, \ldots, k_m$ de $\mathscr{F}$, no todos iguales a z, tales que

$$\sum k_i\xi_i = k_1\xi_1 + k_2\xi_2 + \cdots + k_m\xi_m = \zeta$$

Un conjunto no vacio $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ de vectores de V sobre $\mathscr{F}$ se dice *linealmente independiente* sobre $\mathscr{F}$ si, y solo si,

$$\sum k_i\xi_i = k_1\xi_1 + k_2\xi_2 + \cdots + k_m\xi_m = \zeta$$

implica que *todo* $k_i = z$.

Nota. Una vez fijado el cuerpo $\mathscr{F}$ se omitirá en lo sucesivo la frase «sobre $\mathscr{F}$»; además, por «espacio vectorial $V_n(Q)$», entenderemos el espacio vectorial $V_n(Q)$ sobre Q, y análogamente para $V_n(R)$. Asimismo, si el cuerpo es Q o R, denotaremos el vector nulo por 0. Si bien esto da a 0 otro sentido, siempre se entenderá claramente por el contexto si se trata de un elemento del cuerpo o de un vector del espacio.

Ejemplo 5: (*a*) Los vectores $\xi_1 = (1, 2, 1)$ y $\xi_2 = (3, 1, 5)$ del Ejemplo 4 son linealmente independientes, ya que si

$$k_1\xi_1 + k_2\xi_2 = (k_1 + 3k_2, 2k_1 + k_2, k_1 + 5k_2) = 0 = (0, 0, 0)$$

entonces $k_1 + 3k_2 = 0$, $2k_1 + k_2 = 0$, $k_1 + 5k_2 = 0$. Despejando de la primera relación $k_1 = -3k_2$ y sustituyendo en la segunda, se tiene $-5k_2 = 0$; entonces $k_2 = 0$ y $k_1 = -3k_2 = 0$.

(*b*) Los vectores $\xi_1 = (1, 2, 1)$, $\xi_2 = (3, 1, 5)$ y $\xi_3 = (3, -4, 7)$ son linealmente dependientes, pues $3\xi_1 - 2\xi_2 + \xi_3 = 0$.

Se tiene, en consecuencia,

Teorema IV. Si alguno de los vectores del conjunto $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ de V sobre $\mathscr{F}$ es el vector nulo ζ, S es necesariamente un conjunto linealmente dependiente.

Teorema V. El conjunto de vectores no nulos $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ de V sobre $\mathscr{F}$ es linealmente dependiente si, y solo si, alguno de ellos, por ejemplo, ξ_j, se puede expresar como combinación lineal de los vectores $\xi_1, \xi_2, \ldots, \xi_{j-1}$ que le preceden.

Para una demostración, véase Problema 3.

Teorema VI. Todo subconjunto no vacio de un coujunto de vectores lincalmente independientes es linealmcnte independiente.

Teorema VII. Todo conjunto finito S de vectores, no todos nulos, contiene un subconjunto linealmente independiente U que genera el mismo espacio vectorial que S.

Para una demostración, véase Problema 4.

Ejemplo 6: En el conjunto $S = \{\xi_1, \xi_2, \xi_3\}$ del Ejemplo 5(*b*), ξ_1 y ξ_2 son linealmente independientes, mientras que $\xi_3 = 2\xi_2 - 3\xi_1$. Así, pues, $T_1 = \{\xi_1, \xi_2\}$ es un subconjunto máximo linealmente independiente de S. Pero como $\xi_1 \neq \xi_3$ son linealmente independientes (demostrarlo), en tanto que $\xi_2 = \frac{1}{2}(\xi_3 + 3\xi_1)$, entonces $T_2 = \{\xi_1, \xi_3\}$ es también un subconjunto máximo linealmente independiente de S. Análogamente, $T_3 = \{\xi_2, \xi_3\}$ es otro subconjunto semejante. Por el Teorema VII, cada uno de los subconjuntos T_1, T_2, T_3 genera el mismo espacio que S.

El problema de determinar si un conjunto dado de vectores es lincalmente dependiente o linealmcnte independiente (y dado el caso de dependencia lineal, el de elegir un subconjunto máximo de vectores linealmente independientes) implica a lo sumo estudiar ciertos sistemas de ecuaciones lineales, cosa que si no es difícil, sí puede ser en extremo tediosa. Vamos a dejar los más de estos problemas hasta el Capitulo 14, cuando se expondrá un procedimiento más expeditivo.

Véase Problema 5.

BASES DE UN ESPACIO VECTORIAL

Un conjunto $S = \{\xi_1, \xi_2, \ldots, \xi_n\}$ de vectores de un espacio vectorial V sobre $\mathscr{F}$ se dice una *base* de V si:

(i) S es un conjunto linealmente independiente,

(ii) los vectores de S generan a V.

Definanse los *vectores unitarios* de $V_n(\mathscr{F})$ como sigue:

$$\begin{aligned}
\epsilon_1 &= (u, 0, 0, 0, \ldots, 0, 0) \\
\epsilon_2 &= (0, u, 0, 0, \ldots, 0, 0) \\
\epsilon_3 &= (0, 0, u, 0, \ldots, 0, 0) \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\epsilon_n &= (0, 0, 0, 0, \ldots, 0, u)
\end{aligned}$$

y considérese la combinación lineal

$$\xi = a_1\epsilon_1 + a_2\epsilon_2 + \cdots + a_n\epsilon_n = (a_1, a_2, \ldots, a_n), \quad a_i \in \mathscr{F} \tag{1}$$

Si $\xi = \zeta$, entonces $a_1 = a_2 = \cdots = a_n = z$; de modo que $E = \{\epsilon_1, \epsilon_2, \ldots, \epsilon_n\}$ es un conjunto linealmente independiente. Así que si ξ es un vector cualquiera de $V_n(\mathscr{F})$, entonces (1) lo expresa como combinación lineal de los vectores unitarios. De modo que E genera a $V_n(\mathscr{F})$ y es una base.

Ejemplo 7: Una base de $V_4(R)$ es la base unitaria

$$E = \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\}$$

Otra base es

$$F = \{(1,1,1,0), (0,1,1,1), (1,0,1,1), (1,1,0,1)\}$$

Para demostrar esto, considérese la combinación lineal

$$\begin{aligned}
\xi &= a_1(1,1,1,0) + a_2(0,1,1,1) + a_3(1,0,1,1) + a_4(1,1,0,1) \\
&= (a_1 + a_3 + a_4,\ a_1 + a_2 + a_4,\ a_1 + a_2 + a_3,\ a_2 + a_3 + a_4); \quad a_i \in R
\end{aligned}$$

Si ξ es un vector cualquiera $(p, q, r, s) \in V_4(R)$, hallamos que

$$\begin{aligned}
a_1 &= (p + q + r - 2s)/3 & a_3 &= (p + r + s - 2q)/3 \\
a_2 &= (q + r + s - 2p)/3 & a_4 &= (p + q + s - 2r)/3
\end{aligned}$$

Así que F es un conjunto linealmente independiente (demuéstrese) y genera a $V_4(R)$.

En el Problema 6 se demuestra el

Teorema VIII. Si $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ es una base del espacio vectorial V sobre $\mathscr{F}$ y $T = \{\eta_1, \eta_2, \ldots, \eta_n\}$ es cualquier conjunto linealmente independiente de vectores de V, entonces $n \leq m$.

Como consecuencias tenemos

Teorema IX. Si $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ es una base de V sobre $\mathscr{F}$, entonces cualesquiera $m + 1$ vectores de V forman necesariamente un conjunto linealmente dependiente.

y

Teorema X. Todas las bases de un espacio vectorial V sobre $\mathscr{F}$ tienen el mismo número de elementos.

El número definido en el Teorema X se llama *dimensión* de V. Es evidente que dimensión, como se define aquí, implica dimensión *finita*. No todo espacio vectorial tiene dimensión finita, como se ve en el

Ejemplo 8: (*a*) Por el Ejemplo 7 se sigue que $V_4(R)$ tiene dimensión 4.

(*b*) Considérese $V = \{a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 : a_i \in R\}$
Es claro que $B = \{1, x, x^2, x^3, x^4\}$ es una base y que V tiene dimensión 5.

(*c*) El espacio vectorial V de todos los polinomios en x sobre R no tiene base finita y, por tanto, carece de dimensión. Porque supóngase que B, formado de p polinomios linealmente independientes de V de grados $\leq q$, fuera una base. Como ningún polinomio de V de grado $> q$ puede ser generado por B, no es ésta una base. Véase Problema 7.

SUBESPACIOS DE UN ESPACIO VECTORIAL

Sea V, de dimensión n, un espacio vectorial sobre $\mathscr{F}$ y U, de dimensión $m < n$ del cual $B = \{\xi_1, \xi_2, \ldots, \xi_m\}$ es una base, un subespacio de V. Por el Teorema VIII, solo m de los vectores unitarios de V pueden expresarse como combinaciones lineales de los elementos de B; luego existen vectores de V que no están en U. Sea η_1 uno de esos vectores y considérese

$$k_1\xi_1 + k_2\xi_2 + \cdots + k_m\xi_m + k\eta_1 = \zeta, \qquad k_i,\ k \in \mathscr{F} \tag{2}$$

Ahora bien, $k = z$, pues si no, con $k^{-1} \in \mathscr{F}$,

$$\eta_1 = k^{-1}(-k_1\xi_1 - k_2\xi_2 - \cdots - k_m\xi_m)$$

y $\eta \in U$ en contra de la definición de η_1. Con $k = z$, (2) exige que todo $k_i = z$ puesto que B es una base, y así hemos demostrado el

Teorema XI. Si $B = \{\xi_1, \xi_2, \ldots, \xi_m\}$ es una base de $U \subset V$ y si $\eta_1 \in V$ pero $\eta_1 \notin U$, entonces $B \cup \{\eta_1\}$ es un conjunto linealmente independiente.

Si en el Teorema XI, $m + 1 = n$, la dimensión de V, $B_1 = B \cup \{\eta_1\}$ es una base de V; si $m + 1 < n$, B_1 es una base de cierto subespacio U_1 de V. En este caso, hay un vector η_2 de V pero no de U_1 tal que el espacio U_2 que tiene por base $B \cup \{\eta_1, \eta_2\}$ o bien es V o está propiamente contenido en V, ... Con lo que se obtiene el

Teorema XII. Si $B = \{\xi_1, \xi_2, \ldots, \xi_m\}$ es una base de $U \subset V$ de dimensión n, existen vectores η_1, $\eta_2, \ldots, \eta_{n-m}$ en V tales que $B \cup \{\eta, \eta_2, \ldots, \eta_{n-m}\}$ es una base de V.

Véase Problema 8.

Sean U y W subespacios de V. Definidos

$$U \cap W = \{\xi:\ \xi \in U,\ \xi \in W\}$$

$$U + W = \{\xi + \eta:\ \xi \in U,\ \eta \in W\}$$

y dejamos al lector la demostración de que cada uno de éstos es un subespacio de V.

Ejemplo 9: Considérese $V = V_4(R)$ sobre R con vectores unitarios ϵ_1, ϵ_2, ϵ_3, ϵ_4 como en el Ejemplo 7. Sean

$$U = \{a_1\epsilon_1 + a_2\epsilon_2 + a_3\epsilon_3:\ a_i \in R\}$$

y

$$W = \{b_1\epsilon_2 + b_2\epsilon_3 + b_3\epsilon_4:\ b_i \in R\}$$

subespacios de dimensión 3 de V. Es claro que

$$U \cap W = \{c_1\epsilon_2 + c_2\epsilon_3:\ c_i \in R\}, \quad \text{de dimensión 2}$$

y

$$U + W = \{a_1\epsilon_1 + a_2\epsilon_2 + a_3\epsilon_3 + b_1\epsilon_2 + b_2\epsilon_3 + b_3\epsilon_4:\ a_i, b_i \in R\}$$
$$= \{d_1\epsilon_1 + d_2\epsilon_2 + d_3\epsilon_3 + d_4\epsilon_4:\ d_i \in R\} = V$$

El Ejemplo 9 ilustra el

Teorema XIII. Si U y W, de dimensiones $r \leq n$ y $s \leq n$ respectivamente, son subespacios de un espacio vectorial V de dimensión n y si $U \cap W$ y $U + W$ son de dimensiones p y t respectivamente, entonces $t = r + s - p$.

Para una demostración, véase Problema 9.

ESPACIOS VECTORIALES SOBRE R

En esta sección limitaremos nuestra atención a espacios vectoriales $V = V_n(R)$ sobre R. Se hace esto por dos razones: (1) nuestro estudio tendrá aplicaciones en geometría y (2) de todos los cuerpos posibles, R presenta el mínimo de dificultades.

Considérense en $V = V_2(R)$ los vectores $\xi = (a_1, a_2)$ y $\eta = (b_1, b_2)$ de la Fig. 13-2. La longitud $|\xi|$ de ξ viene dada por $|\xi| = \sqrt{a_1^2 + a_2^2}$ y la longitud de η por $|\eta| = \sqrt{b_1^2 + b_2^2}$. Por el teorema del coseno tenemos

$$|\xi - \eta|^2 = |\xi|^2 + |\eta|^2 - 2\,|\xi| \cdot |\eta| \cos\theta$$

de donde

$$\cos\theta = \frac{(a_1^2 + a_2^2) + (b_1^2 + b_2^2) - [(a_1 - b_1)^2 + (a_2 - b_2)^2]}{2\,|\xi| \cdot |\eta|} = \frac{a_1 b_1 + a_2 b_2}{|\xi| \cdot |\eta|}$$

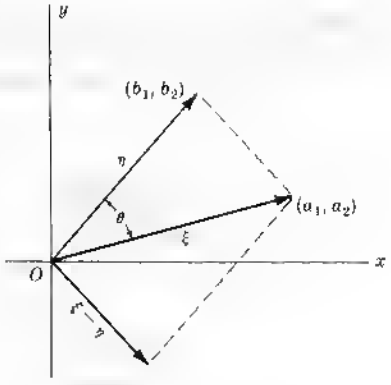


Fig. 13-2

La expresión para $\cos\theta$ sugiere la definición del *producto escalar* (o *producto interno*) de ξ y η por

$$\xi \cdot \eta = a_1 b_1 + a_2 b_2$$

Con lo que $|\xi| = \sqrt{\xi \cdot \xi}$, $\cos\theta = \dfrac{\xi \cdot \eta}{|\xi| \cdot |\eta|}$, y los vectores ξ y η son *ortogonales* (es decir, perpendiculares entre sí, de modo que $\cos\theta = 0$) si, y solo si, $\xi \cdot \eta = 0$.

En el espacio vectorial $V = V_n(R)$ definimos para todo $\xi = (a_1, a_2, \ldots, a_n)$ y $\eta = (b_1, b_2, \ldots, b_n)$,

$$\xi \cdot \eta = \sum a_i b_i = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n$$

$$|\xi| = \sqrt{\xi \cdot \xi} = \sqrt{a_1^2 + a_2^2 + \cdots + a_n^2}$$

De aquí se deduce

(1) $|s\xi| = |s| \cdot |\xi|$ para todo $\xi \in V$ y todo $s \in R$
(2) $|\xi| \geq 0$, la igualdad se verifica solo cuando $\xi = 0$
(3) $|\xi \cdot \eta| \leq |\xi| \cdot |\eta|$ (Desigualdad de Schwarz)
(4) $|\xi + \eta| \leq |\xi| + |\eta|$ (Desigualdad triangular)
(5) ξ y η son ortogonales si, y solo si, $\xi \cdot \eta = 0$.

Para una demostración de (3), véase Problema 10.

Véanse también Problemas 11-13.

Supóngase que en $V_n(R)$ el vector η es ortogonal a cada uno de los $\xi_1, \xi_2, \ldots, \xi_m$. Entonces, como $\eta \cdot \xi_1 = \eta \cdot \xi_2 = \cdots = \eta \cdot \xi_m = 0$, tenemos $\eta \cdot (c_1\xi_1 + c_2\xi_2 + \cdots + c_m\xi_m) = 0$ para cualesquiera $c_i \in R$ y hemos demostrado el

Teorema XIV. Si en $V_n(R)$ un vector η es ortogonal a todo vector del conjunto $\{\xi_1, \xi_2, \ldots, \xi_m\}$, η es ortogonal a todo vector del espacio generado por este conjunto.

Véase Problema 14.

TRANSFORMACIONES LINEALES

Transformación lineal de un espacio vectorial $V(\mathscr{F})$ en un espacio vectorial $W(\mathscr{F})$ sobre el mismo cuerpo $\mathscr{F}$, es una aplicación T de $V(\mathscr{F})$ en $W(\mathscr{F})$ tal que

(i) $(\xi_i + \xi_j)T = \xi_i T + \xi_j T$ para cualesquiera $\xi_i, \xi_j \in V(\mathscr{F})$
(ii) $(s\xi_i)T = s(\xi_i T)$ para cualesquiera $\xi_i \in V(\mathscr{F})$ y $s \in \mathscr{F}$

Limitaremos nuestra atención aquí al caso $W(\mathscr{F}) = V(\mathscr{F})$, es decir, al caso en que T es una aplicación de $V(\mathscr{F})$ en sí mismo. Como la aplicación preserva las operaciones de adición vectorial y multi-

plicación escalar, una transformación lineal de $V(\mathscr{F})$ en sí mismo, o bien es un isomorfismo de $V(\mathscr{F})$ sobre $V(\mathscr{F})$ o bien un homomorfismo de $V(\mathscr{F})$ en $V(\mathscr{F})$.

Ejemplo 10: En geometría analítica plana la conocida rotación de ejes un ángulo α es una transformación lineal

$$T: \quad (x, y) \to (x \cos \alpha - y \operatorname{sen} \alpha,\ x \operatorname{sen} \alpha + y \cos \alpha)$$

de $V_2(R)$ en sí mismo. Como elementos distintos de $V_2(R)$ tienen distintas imágenes y todo elemento es una imagen (demostrarlo), T es un ejemplo de isomorfismo de $V(R)$ sobre sí mismo.

Ejemplo 11: En $V_3(Q)$ considérese la aplicación

$$T: \quad (a, b, c) \to (a + b + 5c,\ a + 2c;\ 2b + 6c), \qquad (a, b, c) \in V_3(Q)$$

Por $(a, b, c), (d, e, f) \in V_3(Q)$ y $s \in Q$, tenemos

(i) $(a, b, c) + (d, e, f) = (a + d, b + e, c + f) \to$

$$(a + d + b + e + 5c + 5f,\ a + d + 2c + 2f,\ 2b + 2e + 6c + 6f)$$
$$= (a + b + 5c,\ a + 2c,\ 2b + 6c) + (d + e + 5f,\ d + 2f,\ 2e + 6f)$$

es decir, $\qquad [(a, b, c) + (d, c, f)]T = (a, b, c)T + (d, e, f)T$

y

(ii) $s(a, b, c) = (sa, sb, sc) \to (sa + sb + 5sc,\ sa + 2sc,\ 2sb + 6sc)$

$$= s(a + b + 5c,\ a + 2c,\ 2b + 6c)$$

es decir, $\qquad [s(a, b, c)]T = s[(a, b, c)T]$

Así que T es una transformación lineal sobre $V_3(Q)$

Como $(0, 0, 1)$ y $(2, 3, 0)$ tienen la misma imagen $(5, 2, 6)$, esta transformación lineal es ejemplo de un homomorfismo de $V_3(Q)$ en sí mismo.

La transformación lineal T del Ejemplo 10 se puede escribir como

$$x(1, 0) + y(0, 1) \to x(\cos \alpha, \operatorname{sen} \alpha) + y(-\operatorname{sen} \alpha, \cos \alpha)$$

lo que sugiere que T puede darse como

$$T: \quad (1, 0) \to (\cos \alpha, \operatorname{sen} \alpha),\ (0, 1) \to (-\operatorname{sen} \alpha, \cos \alpha)$$

Así también, T del Ejemplo 11 se puede escribir como

$$a(1, 0, 0) + b(0, 1, 0) + c(0, 0, 1) \to a(1, 1, 0) + b(1, 0, 2) + c(5, 2, 6)$$

lo que sugiere que T puede darse como

$$T: \quad (1, 0, 0) \to (1, 1, 0),\ (0, 1, 0) \to (1, 0, 2),\ (0, 0, 1) \to (5, 2, 6)$$

De lo que se infiere:

Toda transformación lineal de un espacio vectorial en sí mismo se puede describir completamente expresando el efecto que produce en los vectores unitarios de base del espacio.

Véase Problema 15.

En el Problema 16 se demuestra la propiedad más general

Teorema XV. Si $\{\xi_1, \xi_2, \ldots, \xi_n\}$ es *cualquier* base de $V = V(\mathscr{F})$ y si $\{\eta_1, \eta_2, \ldots, \eta_n\}$ es cualquier conjunto de n elementos de V, la aplicación

$$T: \quad \xi_i \to \eta_i, \quad (i = 1, 2, \ldots, n)$$

define una transformación lineal de V en sí mismo.

En el Problema 17 demostramos el

Teorema XVI. Si T es una transformación lineal de $V(\mathscr{F})$ en si mismo y si W es un subespacio de $V(\mathscr{F})$, entonces $W_T = \{\xi T : \xi \in W\}$, la imagen de W por T, es también un subespacio de $V(\mathscr{F})$.

Volviendo ahora al Ejemplo 11, observamos que las imágenes de los vectores unitarios de base de $V_3(Q)$ son linealmente dependientes, es decir, que $2\epsilon_1 T + 3\epsilon_2 T - \epsilon_3 T = (0, 0, 0,)$. Así, pues, $V_T \subset V$; en efecto, como (1, 1, 0) y (1, 0, 2) son linealmente independientes, V_T tiene dimensión 2. Si definimos la *característica* (o rango) de una transformación lineal T de un espacio vectorial V como la dimensión del espacio imagen V_T de V por T, tenemos por el Teorema XVI,

$$r_T = \text{característica de } T \leq \text{dimensión de } V$$

Cuando vale la igualdad, diremos que la transformación lineal T es *regular*; si no, que T es *singular*. Así que T del Ejemplo 11 es singular de característica 2.

Considérese ahora la transformación lineal T del Teorema XV y supóngase T singular. Como los vectores imagen η_i son entonces linealmente dependientes, hay elementos $s_i \in \mathscr{F}$, no todos s_i, tales que $\sum s_i\eta_i = \zeta$. Entonces, para $\xi = \sum s_i\xi_i$, tenemos $\xi T = \zeta$. Recíprocamente, supóngase $\eta = \sum t_i\xi_i \neq \zeta$ y

$$\eta T = \sum (t_i\xi_i)T = t_1(\xi_1 T) + t_2(\xi_2 T) + \cdots + t_n(\xi_n T) = \zeta$$

Entonces los vectores imagen $\xi_i T$, $(i = 1, 2, \ldots, n)$ deben ser linealmente dependientes. Hemos demostrado así el

Teorema XVII. Una transformación lineal T de un espacio vectorial $V(\mathscr{F})$ es singular si, y solo si, existe un vector no nulo $\xi \in V(\mathscr{F})$ tal que $\xi T = \zeta$.

Ejemplo 12: Para cada una de las siguientes transformaciones lineales de $V_4(Q)$ en si mismo, determinar si es o no singular.

$$(a)\quad A: \begin{cases} \epsilon_1 \to (1,1,0,0) \\ \epsilon_2 \to (0,1,1,0) \\ \epsilon_3 \to (0,0,1,1) \\ \epsilon_4 \to (0,1,0,1) \end{cases} \qquad (b)\quad B: \begin{cases} \epsilon_1 \to (1,1,0,0) \\ \epsilon_2 \to (0,1,1,0) \\ \epsilon_3 \to (0,0,1,1) \\ \epsilon_4 \to (1,1,1,1) \end{cases}$$

Sea $\xi = (a, b, c, d)$ un vector cualquiera de $V_4(Q)$.

(*a*) Hagamos $\xi A = (a\epsilon_1 + b\epsilon_2 + c\epsilon_3 + d\epsilon_4)A = (a,\ a + b + d,\ b + c,\ c + d) = 0$. Como esto exige que $a = b = c = d = 0$, es decir, que $\xi = 0$, A es regular.

(*b*) Hagamos $\xi B = (a + d, a + b + d, b + c + d, c + d) = 0$. Como esto se cumple si $a = c = 1$, $b = 0$, $d = -1$, tenemos $(1, 0, 1, -1)B = 0$ y B es singular, cosa evidente a simple vista, es decir, $\epsilon_1 B + \epsilon_3 B = \epsilon_4 B$. Entonces, como $\epsilon_1 B$, $\epsilon_2 B$, $\epsilon_3 B$ son linealmente independientes como es manifiesto, B tiene característica 3 y es singular.

Dejaremos nuevamente (véase el párrafo que sigue al Ejemplo 6) otros ejemplos y problemas para el Capítulo 14.

ALGEBRA DE LAS TRANSFORMACIONES LINEALES

Denótese por $\mathscr{A}$ el conjunto de todas las transformaciones lineales de un espacio vectorial dado $V(\mathscr{F})$ sobre $\mathscr{F}$ en si mismo y por $\mathscr{M}$ el conjunto de todas las transformaciones lineales no singulares de $\mathscr{A}$. Definanse adición $(+)$ y multiplicación $(\cdot)$ sobre $\mathscr{A}$ por

$$A + B: \quad \xi(A + B) = \xi A + \xi B, \qquad \xi \in V(\mathscr{F})$$

y

$$A \cdot B: \quad \xi(A \cdot B) = (\xi A)B, \qquad \xi \in V(\mathscr{F})$$

para todo $A, B \in \mathscr{A}$. Defínase una multiplicación escalar sobre $\mathscr{A}$ por

$$kA: \quad \xi(kA) = (k\xi)A, \qquad \xi \in V(\mathscr{F})$$

para todo $A \in \mathscr{A}$ y $k \in \mathscr{F}$.

Ejemplo 13: Sean

$$A: \begin{cases} \epsilon_1 \to (a, b) \\ \epsilon_2 \to (c, d) \end{cases} \qquad \text{y} \qquad B: \begin{cases} \epsilon_1 \to (e, f) \\ \epsilon_2 \to (g, h) \end{cases}$$

transformaciones lineales de $V_2(R)$ en sí mismo. Para cualquier vector $\xi = (s, t) \in V_2(R)$, encontramos

$$\begin{aligned} \xi A &= (s, t)A = (s\epsilon_1 + t\epsilon_2)A = s(a, b) + t(c, d) \\ &= (sa + tc, sb + td) \end{aligned}$$

$$\xi B = (se + tg, sf + th)$$

y

$$\xi(A + B) = (s, t)A + (s, t)B = \big(s(a + e) + t(c + g), s(b + f) + t(d + h)\big)$$

Así, pues, tenemos

$$A + B: \begin{cases} \epsilon_1 \to (a + e, b + f) \\ \epsilon_2 \to (c + g, d + h) \end{cases}$$

De igual modo,

$$\begin{aligned} \xi(A \cdot B) &= \big((s, t)A\big)B = (sa + tc, sb + td)B \\ &= (sa + tc) \cdot (e, f) + (sb + td) \cdot (g, h) \\ &= \big(s(ae + bg) + t(ce + dg), s(af + bh) + t(cf + dh)\big) \end{aligned}$$

y

$$A \cdot B: \begin{cases} \epsilon_1 \to (ae + bg, af + bh) \\ \epsilon_2 \to (ce + dg, cf + dh) \end{cases}$$

Por último, para cualquier $k \in R$, hallamos

$$(k\xi)A = (ks, kt)A = \big(k(sa + tc), k(sb + td)\big)$$

y

$$kA: \begin{cases} \epsilon_1 \to (ka, kb) \\ \epsilon_2 \to (kc, kd) \end{cases}$$

En el Ejercicio 18 demostramos el

Teorema XVIII. El conjunto $\mathscr{A}$ de todas las transformaciones lineales de un espacio vectorial en sí mismo forma un anillo con respecto a la adición y multiplicación anteriormente definidas.

En el Ejercicio 19, demostramos el

Teorema XIX. El conjunto $\mathscr{M}$ de todas las transformaciones lineales no singulares de un espacio vectorial en sí mismo forma un grupo con respecto a la multiplicación.

Dejamos al lector el demostrar el

Teorema XX. Si $\mathscr{A}$ es el conjunto de todas las transformaciones lineales de un espacio vectorial $V(\mathscr{F})$ sobre $\mathscr{F}$ en sí mismo, entonces $\mathscr{A}$ es a su vez un espacio vectorial sobre $\mathscr{F}$.

Sean, $A, B \in \mathscr{A}$. Como para todo $\xi \in V$,

$$\xi(A + B) = \xi A + \xi B$$

es evidente que

$$V_{(A+B)} \subseteq V_A + V_B$$

Entonces, dimensión de $V_{(A+B)} \leq$ dimensión de V_A + dimensión de V_B

y

$$r_{(A+B)} \leq r_A + r_B$$

Como para cualquier transformación lineal $T \in \mathscr{A}$,

$$\text{dimensión de } V_T \leq \text{dimensión de } V$$

tenemos $\quad \text{dimensión de } V_{(A\cdot B)} \leq \text{dimensión de } V_A$

Así mismo, como $V_A \subseteq V$, $\quad \text{dimensión de } V_{(A\cdot B)} \leq \text{dimensión de } V_B$

De modo que $\quad r_{(A\cdot B)} \leq r_A, \qquad r_{(A\cdot B)} \leq r_B$

Problemas resueltos

1. Demostrar: Un conjunto no vacío U de un espacio vectorial V sobre $\mathscr{F}$ es un subespacio de V si, y solo si, U es cerrado con respecto a la multiplicación escalar y a la adición vectorial definidas sobre V.

Supóngase que U es un subespacio de V; entonces U es cerrado con respecto a la multiplicación escalar y a la adición vectorial. Recíprocamente, supóngase que U es un subconjunto no vacío de V, cerrado respecto de la multiplicación escalar y adición vectorial. Sea $\xi \in U$; entonces $(-u)\xi = -(u\xi) = -\xi \in U$ y $\xi + (-\xi) = \zeta \in U$. Así, pues, U es un grupo aditivo abeliano. Como las propiedades (i)-(iv), página 144, son válidas en V, también lo son en U. De modo que U es un espacio vectorial sobre $\mathscr{F}$ y, por consiguiente, es un subespacio de V.

2. En el espacio vectorial $V_3(R)$ sobre R (Ejemplo 3, página 145), sean U generado por $\xi_1 = (1, 2, -1)$ y $\xi_2 = (2, -3, 2)$ y W generado por $\xi_3 = (4, 1, 3)$ y $\xi_4 = (-3, 1, 2)$. ¿Son U y W idénticos subespacios de V?

Primero considérese el vector $\xi = \xi_3 - \xi_4 = (7, 0, 1) \in W$ y el vector

$$\eta = x\xi_1 + y\xi_2 = (x + 2y,\ 2x - 3y,\ -x + 2y) \in U$$

Entonces, ξ y η son los mismos si existen $x, y \in R$ tales que

$$(x + 2y,\ 2x - 3y,\ -x + 2y) = (7, 0, 1)$$

Encontramos que $x = 3$, $y = 2$. En realidad esto no demuestra que U y W son idénticos; para eso tenemos que poder encontrar $x, y \in R$ tales que

$$x\xi_1 + y\xi_2 = a\xi_3 + b\xi_4$$

para $a, b \in R$ cualesquiera.

De $\begin{cases} x + 2y = 4a - 3b \\ -x + 2y = 3a + 2b \end{cases}$ obtenemos $x = \frac{1}{2}(a - 5b)$, $y = \frac{1}{4}(7a - b)$. Como $2x - 3y \neq a + b$; U y W no son idénticos.

Geométricamente, U y W son planos diferentes que pasan por O, el origen de coordenadas en el espacio ordinario. Tienen, desde luego, una recta de vectores en común, siendo uno de estos vectores comunes el (7, 0, 1).

3. Demostrar: El conjunto de vectores no nulos $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ de V sobre $\mathscr{F}$ es linealmente dependiente si, y solo si, alguno de ellos, ξ_j, se puede expresar como combinación lineal de los vectores $\xi_1, \xi_2, \ldots, \xi_{j-1}$ que le preceden.

Supóngase que los m vectores son linealmente dependientes de modo que existen escalares $k_1, k_2, \ldots, k_m$, no todos iguales a z, tales que $\sum k_i\xi_i = \zeta$. Supóngase además que el coeficiente k_j no es z en tanto que los coeficientes $k_{j+1}, k_{j+2}, \ldots, k_m$ son z (sin excluir naturalmente el caso extremo $j = m$). Entonces, en efecto,

$$k_1\xi_1 + k_2\xi_2 + \cdots + k_j\xi_j = \zeta \qquad (1)$$

y como $k_j\xi_j \neq \zeta$, tenemos

$$k_j\xi_j = -k_1\xi_1 - k_2\xi_2 - \cdots - k_{j-1}\xi_{j-1}$$

o bien

$$\xi_j = q_1\xi_1 + q_2\xi_2 + \cdots + q_{j-1}\xi_{j-1} \tag{2}$$

con alguno de los $q_i \neq z$. Así que ξ_j es una combinación lineal de los vectores que le preceden.

Recíprocamente, supóngase que se verifica (2). Entonces,

$$k_1\xi_1 + k_2\xi_2 + \cdots + k_j\xi_j + z\xi_{j+1} + z\xi_{j+2} + \cdots + z\xi_m = \zeta$$

con $k_j \neq z$ y los vectores $\xi_1, \xi_2, \ldots, \xi_m$ son linealmente dependientes.

4. Demostrar: Todo conjunto finito S de vectores, no todos nulos, contiene un subconjunto U linealmente independiente que genera el mismo espacio que S.

Sea $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$. La discusión hecha hasta ahora indica que U existe, en tanto que el Teorema V sugiere el procedimiento siguiente para obtenerlo a partir de S. Considerando sucesivamente cada vector de izquierda a derecha, convengamos en excluir todo vector que (1) sea el vector nulo, o (2) se pueda escribir como combinación lineal de todos los que le preceden. Supóngase que hay $n \leq m$ vectores que quedan y denotémoslos ahora de otra manera escribiendo $U = \{\eta_1, \eta_2, \ldots, \eta_n\}$. Por su construcción, U es un subconjunto linealmente independiente de S que genera el mismo espacio que S.

El Ejemplo 6, página 146, muestra, como se hubiera podido anticipar, que habrá usualmente subconjuntos de S linealmente independientes, distintos de U, que generarán el mismo espacio que S. Una ventaja del procedimiento utilizado arriba es que, una vez puestos los elementos de S en un cierto orden, solo se puede formar un subconjunto, el U, que sea linealmente independiente.

5. Hallar un subconjunto U linealmente independiente del conjunto $S = \{\xi_1, \xi_2, \xi_3, \xi_4\}$, siendo

$$\xi_1 = (1, 2, -1),\ \xi_2 = (-3, -6, 3),\ \xi_3 = (2, 1, 3),\ \xi_4 = (8, 7, 7) \in R,$$

que genere el mismo espacio que S.

Primero, notamos que $\xi_1 \neq \zeta$ y pasamos a ξ_2. Como $\xi_2 = -3\xi_1$ (es decir, ξ_2 es una combinación lineal de ξ_1), Excluimos ξ_2 y pasamos a ξ_3. Entonces, es $\xi_3 \neq s\xi_1$, para todo $s \in R$; pasamos a ξ_4. Como ξ_4 no es múltiplo escalar de ξ_1 ni de ξ_3 (y, por tanto, nó queda excluido automáticamente), ponemos

$$s\xi_1 + t\xi_3 = s(1, 2, -1) + t(2, 1, 3) = (8, 7, 7) = \xi_4$$

y buscamos una solución en R, si existe, del sistema

$$s + 2t = 8,\quad 2s + t = 7,\quad -s + 3t = 7$$

El lector verificará que $\xi_4 = 2\xi_1 + 3\xi_3$; luego, $U = \{\xi_1, \xi_3\}$ es el subconjunto pedido.

6. Demostrar: Si $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ es una base de un espacio vectorial V sobre $\mathscr{F}$ y si $T = \{\eta_1, \eta_2, \ldots, \eta_n\}$ es un conjunto linealmente independiente de vectores de V, entonces $n \leq m$.

Como todo elemento de T se puede escribir como combinación lineal de los elementos base, el conjunto

$$S' = \{\eta_1, \xi_1, \xi_2, \ldots, \xi_m\}$$

genera V y es linealmente dependiente. Ahora bien, $\eta_1 \neq \zeta$; por tanto, alguno de los ξ debe ser combinación lineal de los elementos que le preceden en S'. Examinando sucesivamente los ξ, supóngase que hallamos que ξ_i cumple esta condición. Excluyendo a ξ_i de S', tenemos el conjunto

$$S_1 = \{\eta_1, \xi_1, \xi_2, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_m\}$$

que es una base de V como vamos a demostrarlo. Es claro que S_1 genera el mismo espacio que S', es decir, S_1 genera V. Así que solo necesitamos demostrar que S_1 es un conjunto linealmente independiente. Escribamos

$$\eta_1 = a_1\xi_1 + a_2\xi_2 + \cdots + a_i\xi_i, \qquad a_j \in \mathscr{F},\ a_i \neq z$$

Si S_1 fuera un conjunto linealmente dependiente, habria algún ξ_j, $j > i$, que se podria expresar asi:

$$\xi_j = b_1\eta_1 + b_2\xi_1 + b_3\xi_2 + \cdots + b_i\xi_{i-1} + b_{i+1}\xi_{i+1} + \cdots + b_{j-1}\xi_{j-1}, \quad b_1 \neq z$$

de donde, sustituyendo η_1,

$$\xi_j = c_1\xi_1 + c_2\xi_2 + \cdots + c_{j-1}\xi_{j-1}$$

contra lo supuesto de que S es un conjunto linealmente independiente.

Análogamente, $S_1' = \{\eta_2, \eta_1, \xi_1, \xi_2, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_m\}$

es un conjunto linealmente dependiente que genera a V. Como η_1 y η_2 son linealmente independientes, alguno de los ξ de S_1', ξ_j, por ejemplo, es combinación lineal de todos los vectores que le preceden. Reiterando el razonamiento anterior, se obtiene (suponiendo $j > i$) el conjunto

$$S_2 = \{\eta_2, \eta_1, \xi_1, \xi_2, \ldots, \xi_{i-1}, \xi_{i+1}, \ldots, \xi_{j-1}, \xi_{j+1}, \ldots, \xi_m\}$$

como base de V.

Pero este proceso se puede repetir hasta agotar T con tal que $n \leq m$. Supóngase $n > m$ y que hemos obtenido

$$S_m = \{\eta_m, \eta_{m-1}, \ldots, \eta_2, \eta_1\}$$

como base de V. Considérese $S_m' = S \cup \{\eta_{m+1}\}$. Como S_m es una base de V y $\eta_{m+1} \in V$, entonces η_{m+1} es combinación lineal de los vectores de S_m. Pero esto contradice la hipótesis sobre T. Luego $n \leq m$, como se requiere.

7. (*a*) Elegir una base de $V_3(R)$ del conjunto

$$S = \{\xi_1, \xi_2, \xi_3, \xi_4\} = \{(1, -3, 2), (2, 4, 1), (3, 1, 3), (1, 1, 1)\}$$

(*b*) Expresar los vectores unitarios de $V_3(R)$ como combinaciones lineales de los vectores de base encontrados en (*a*).

(*a*) Si el problema tiene solución, alguno de los ξ debe ser combinación lineal de los que le preceden. Se ve de inmediato que $\xi_3 = \xi_1 + \xi_2$. Para demostrar que $\{\xi_1, \xi_2, \xi_4\}$ es un conjunto linealmente independiente y que, por tanto, es la base pedida, tenemos que demostrar que

$$a\xi_1 + b\xi_2 + c\xi_4 = (a + 2b + c, -3a + 4b + c, 2a + b + c) = (0, 0, 0)$$

implica $a = b = c = 0$. Se deja esto al lector.

El mismo resultado se obtiene demostrando que

$$s\xi_1 + t\xi_2 = \xi_4, \qquad s, t \in R$$

es decir, que $\begin{cases} s + 2t = 1 \\ -3s + 4t = 1 \\ 2s + t = 1 \end{cases}$ es imposible. Por último, el lector familiarizado con los determinantes recordará que estas ecuaciones tienen solución si, y solo si, $\begin{vmatrix} 1 & 2 & 1 \\ -3 & 4 & 1 \\ 2 & 1 & 1 \end{vmatrix} = 0$.

(*b*) Hágase $a\xi_1 + b\xi_2 + c\xi_4$ igual a los vectores unitarios ϵ_1, ϵ_2, ϵ_3 sucesivamente obteniendo

$$\begin{cases} a + 2b + c = 1 \\ -3a + 4b + c = 0 \\ 2a + b + c = 0 \end{cases} \qquad \begin{cases} a + 2b + c = 0 \\ -3a + 4b + c = 1 \\ 2a + b + c = 0 \end{cases} \qquad \begin{cases} a + 2b + c = 0 \\ -3a + 4b + c = 0 \\ 2a + b + c = 1 \end{cases}$$

siendo las soluciones:

$$a = 3/2,\ b = 5/2,\ c = -11/2 \qquad a = b = -1/2,\ c = 3/2 \qquad a = -1,\ b = -2,\ c = 5$$

Así, pues, $\epsilon_1 = \frac{1}{2}(3\xi_1 + 5\xi_2 - 11\xi_4)$, $\epsilon_2 = \frac{1}{2}(-\xi_1 - \xi_2 + 3\xi_4)$, y $\epsilon_3 = -\xi_1 - 2\xi_2 + 5\xi_4$.

Determinar, si es posible, una base del espacio vectorial $V_4(Q)$ que incluya los vectores $\xi_1 = (3, -2, 0, 0)$ y $\xi_2 = (0, 1, 0, 1)$.

Como $\xi_1 \neq \zeta$, $\xi_2 \neq \zeta$ y $\xi_2 \neq s\xi_1$, para todo $s \in Q$, sabemos que ξ_1 y ξ_2 pueden ser elementos de una base de $V_4(Q)$. Como los vectores unitarios $\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4$ (véase Ejemplo 7, página 147) son una base de $V_4(Q)$, el con-

junto $S = \{\xi_1, \xi_2, \epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4\}$ genera a $V_4(Q)$ y contiene seguramente una base del tipo que buscamos. Ahora bien, ϵ_1 será un elemento de la base dicha si, y solo si,

$$a\xi_1 + b\xi_2 + c\epsilon_1 = (3a + c, -2a + b, 0, b) = (0, 0, 0, 0)$$

implica $a = b = c = 0$. Evidentemente, ϵ_1 puede servir como elemento de la base. Y nuevamente, ϵ_2 será un elemento si, y solo si,

$$a\xi_1 + b\xi_2 + c\epsilon_1 + d\epsilon_2 = (3a + c, -2a + b + d, 0, b) = (0, 0, 0, 0) \qquad (1)$$

implica $a = b = c = d = 0$. Tenemos $b = 0 = 3a + c = -2a + d$; entonces, (1) se verifica para $a = 1$, $b = 0$, $c = -3$, $d = 2$, y entonces $\{\xi_1, \xi_2, \epsilon_1, \epsilon_2\}$ no es una base. Dejamos al lector comprobar que $\{\xi_1, \xi_2, \epsilon_1, \epsilon_3\}$ es una base.

9. Demostrar: Si U y W, de dimensiones $r \leq n$ y $s \leq n$ respectivamente son subespacios de un espacio vectorial V de dimensión n y si $U \cap W$ y $U + W$ son de dimensiones p y t respectivamente, entonces $t = r + s - p$.

Tómese $A = \{\xi_1, \xi_2, \ldots, \xi_p\}$ como base de $U \cap W$ y, según el Teorema XII, página 148, tómese $B = A \cup \{\lambda_1, \lambda_2, \ldots, \lambda_{r-p}\}$ como base de U y $C = A \cup \{\mu_1, \mu_2, \ldots, \mu_{s-p}\}$ como base de W. Entonces, por definición, todo vector de $U + W$ se puede expresar como combinación lineal de los vectores de

$$D = \{\xi_1, \xi_2, \ldots, \xi_p, \lambda_1, \lambda_2, \ldots, \lambda_{r-p}, \mu_1, \mu_2, \ldots, \mu_{s-p}\}$$

Para demostrar que D es un conjunto linealmente independiente y que, por tanto, es una base de $U + W$, considérese

$$a_1\xi_1 + a_2\xi_2 + \cdots + a_p\xi_p + b_1\lambda_1 + b_2\lambda_2 + \cdots + b_{r-p}\lambda_{r-p} + c_1\mu_1 + c_2\mu_2 + \cdots + c_{s-p}\mu_{s-p} = \zeta \qquad (1)$$

donde $a_i, b_j, c_k \in \mathscr{F}$.

Hágase $\pi = c_1\mu_1 + c_2\mu_2 + \cdots + c_{s-p}\mu_{s-p}$. Como $\pi \in W$ y por (1) $\pi \in U$, es $\pi \in U \cap W$ y es combinación lineal de los vectores de A, sea $\pi = d_1\xi_1 + d_2\xi_2 + \cdots + d_p\xi_p$. Entonces,

$$c_1\mu_1 + c_2\mu_2 + \cdots + c_{s-p}\mu_{s-p} - d_1\xi_1 - d_2\xi_2 - \cdots - d_p\xi_p = \zeta$$

y, como C es una base de W, cada $c_i = z$ y cada $d_i = z$. Con cada $c_i = z$, (1) se convierte en

$$a_1\xi_1 + a_2\xi_2 + \cdots + a_p\xi_p + b_1\lambda_1 + b_2\lambda_2 + \cdots + b_{r-p}\lambda_{r-p} = \zeta \qquad (1')$$

Como B es una base de U, cada $a_i = z$ y cada $b_i = z$ en (1'). Entonces D es un conjunto linealmente independiente y, por tanto, es una base de $U + W$ de dimensión $t = r + s - p$.

10. Demostrar: $|\xi \cdot \eta| \leq |\xi| \cdot |\eta|$ para cualesquiera $\xi, \eta \in V_n(R)$.

Para $\xi = 0$ o $\eta = 0$, tenemos $0 \leq 0$. Supóngase $\xi \neq 0$ y $\eta \neq 0$; entonces, $|\eta| = k|\xi|$ para algún $k \in R^+$, y tenemos

$$\eta \cdot \eta = |\eta|^2 = [k \cdot |\xi|]^2 = k \cdot |\xi| \cdot |\eta| = k^2 \cdot |\xi|^2 = k^2(\xi \cdot \xi)$$

y

$$0 \leq (k\xi \pm \eta) \cdot (k\xi \pm \eta) = k^2(\xi \cdot \xi) \pm 2k(\xi \cdot \eta) + \eta \cdot \eta$$
$$= 2k \cdot |\xi| \cdot |\eta| \pm 2k(\xi \cdot \eta)$$

Luego

$$\pm 2k(\xi \cdot \eta) \leq 2k|\xi| \cdot |\eta|$$
$$\pm(\xi \cdot \eta) \leq |\xi| \cdot |\eta|$$

y

$$|\xi \cdot \eta| \leq |\xi| \cdot |\eta|$$

11. Dados $\xi = (1, 2, 3, 4)$ y $\eta = (2, 0, -3, 1)$, hallar

(a) $\xi \cdot \eta$, (b) $|\xi|$ y $|\eta|$, (c) $|5\xi|$ y $|-3\eta|$, (d) $|\xi + \eta|$

(a) $\xi \cdot \eta = 1 \cdot 2 + 2 \cdot 0 + 3(-3) + 4 \cdot 1 = -3$

(b) $|\xi| = \sqrt{1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 + 4 \cdot 4} = \sqrt{30}$, $\quad |\eta| = \sqrt{4 + 9 + 1} = \sqrt{14}$

(c) $|5\xi| = \sqrt{25 + 25 \cdot 4 + 25 \cdot 9 + 25 \cdot 16} = 5\sqrt{30}$, $\quad |-3\eta| = \sqrt{9 \cdot 4 + 9 \cdot 9 + 9 \cdot 1} = 3\sqrt{14}$

(d) $\xi + \eta = (3, 2, 0, 5)$ y $|\xi + \eta| = \sqrt{9 + 4 + 25} = \sqrt{38}$

12. Dados $\xi = (1, 1, 1)$ y $\eta = (3, 4, 5)$ de $V_3(R)$, hallar el vector más corto de la forma $\lambda = \xi + s\eta$.

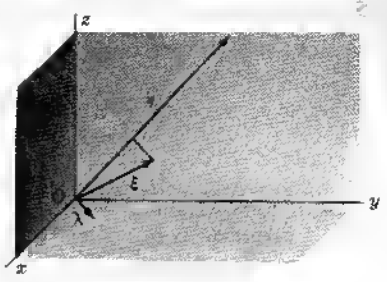


Fig. 13-3

Aquí es $\lambda = (1+3s, 1+4s, 1+5s)$

y $|\lambda|^2 = 3 + 24s + 50s^2$

Ahora bien, $|\lambda|$ es mínimo cuando $24 + 100s = 0$. Luego $\lambda = (7/25, 1/25, -1/5)$. Se encuentra fácilmente que λ y η son ortogonales. Hemos resuelto así el problema de hallar la mínima distancia del punto $P(1, 1, 1)$ del espacio ordinario a la recta que va del origen a $Q(3, 4, 5)$.

13. Para $\xi = (a_1, a_2, a_3)$, $\eta = (b_1, b_2, b_3) \in V_3(R)$, defínase

$$\xi \times \eta = (a_2b_3 - a_3b_2,\ a_3b_1 - a_1b_3,\ a_1b_2 - a_2b_1)$$

(*a*) Demostrar que $\xi \times \eta$ es ortogonal a ξ y a η.

(*b*) Hallar un vector λ ortogonal a $\xi = (1, 1, 1)$ y a $\eta = (1, 2, -3)$.

(*a*) $\xi \cdot (\xi \times \eta) = a_1(a_2b_3 - a_3b_2) + a_2(a_3b_1 - a_1b_3) + a_3(a_1b_2 - a_2b_1) = 0$ y análogamente para $\eta \cdot (\xi \times \eta)$.

(*b*) $\lambda = \xi \times \eta = \big(1(-3) - 2 \cdot 1,\ 1 \cdot 1 - 1(-3),\ 1 \cdot 2 - 1 \cdot 1\big) = (-5, 4, 1)$

14. Sean $\xi = (1, 1, 1, 1)$ y $\eta = (1, 2, -3, 0)$ vectores dados de $V_4(R)$.

(*a*) Demostrar que son ortogonales.

(*b*) Hallar dos vectores linealmente independientes λ y μ, que sean ortogonales tanto a ξ como a η.

(*c*) Hallar un vector v no nulo ortogonal a los ξ, η, λ y demostrar que es combinación lineal de λ y μ.

(*a*) $\xi \cdot \eta = 1 \cdot 1 + 1 \cdot 2 + 1 \cdot (-3) + 0 = 0$; de modo que ξ y η son ortogonales.

(*b*) Supóngase que $(a, b, c, d) \in V_4(R)$ es ortogonal a ξ y a η; entonces,

$$\text{(i)} \qquad a + b + c + d = 0 \qquad \text{y} \qquad a + 2b - 3c = 0$$

Tómese primero $c = 0$. Entonces $a + 2b = 0$ se verifica para $a = 2$, $b = -1$; y $a + b + c + d = 0$ da ahora $d = -1$. Tenemos $\lambda = (2, -1, 0, -1)$.

Tómese después $b = 0$. Entonces $a - 3c = 0$ se cumple para $a = 3$, $c = 1$; y $a + b + c + d = 0$ da ahora $d = -4$. Tenemos $\mu = (3, 0, 1, -4)$. Evidentemente, λ y μ son linealmente independientes.

Como una solución obvia de las ecuaciones (i) es $a = b = c = d = 0$, ¿por qué no se toma $\lambda = (0, 0, 0, 0)$?

(*c*) Si $v = (a, b, c, d)$ es ortogonal a ξ, η y λ, entonces

$$a + b + c + d = 0, \qquad a + 2b - 3c = 0 \qquad \text{y} \qquad 2a - b - d = 0$$

Sumando la primera y última ecuaciones, tenemos $3a + c = 0$, que se cumple para $a = 1$, $c = -3$. Entonces $b = -5$, $d = 7$ y $v = (1, -5, -3, 7)$. Por último, $v = 5\lambda - 3\mu$.

Nota. Téngase en cuenta que las soluciones obtenidas aquí no son únicas. En primer lugar, cualquier múltiplo escalar no nulo de cualesquiera o de todos los λ, μ, v es también una solución. Y además, al determinar λ (y también μ) hemos hecho arbitrariamente $c = 0$ (también $b = 0$). No obstante, examínese la solución en (*c*) y verifíquese que v es único salvo en un factor escalar.

15. Hallar la imagen de $\xi = (1, 2, 3, 4)$ por la transformación lineal

$$A: \begin{cases} \epsilon_1 \to (1,-2,0,4) \\ \epsilon_2 \to (2,4,1,-2) \\ \epsilon_3 \to (0,-1,5,-1) \\ \epsilon_4 \to (1,3,2,0) \end{cases}$$

de $V_4(Q)$ en si mismo.

Tenemos

$$\xi = \epsilon_1 + 2\epsilon_2 + 3\epsilon_3 + 4\epsilon_4 \to$$
$$(1,-2,0,4) + 2(2,4,1,-2) + 3(0,-1,5,-1) + 4(1,3,2,0) = (9, 15, 25, -3)$$

16. Demostrar: Si $\{\xi_1, \xi_2, \ldots, \xi_n\}$ es una base cualquiera de $V = V(\mathscr{F})$ y si $\{\eta_1, \eta_2, \ldots, \eta_n\}$ es cualquier conjunto de n elementos de V, la aplicación

$$T: \quad \xi_i \to \eta_i, \qquad (i = 1, 2, \ldots, n)$$

define una transformación lineal de V en si mismo.

Sean $\xi = \sum s_i\xi_i$ y $\eta = \sum t_i\xi_i$ dos vectores de V. Entonces

$$\xi + \eta = \sum (s_i + t_i)\xi_i \to \sum (s_i + t_i)\eta_i = \sum s_i\eta_i + \sum t_i\eta_i$$

de manera que (i) $\qquad (\xi + \eta)T = \xi T + \eta T$

Así, pues, para cualquier $s \in \mathscr{F}$ y cualquier $\xi \in V$,

$$s\xi = s\sum s_i\xi_i \to s\sum s_i\eta_i$$

de modo que (ii) $\qquad (s\xi)T = s(\xi T)$

según se afirmaba

17. Demostrar: Si T es una transformación lineal de $V(\mathscr{F})$ en sí mismo, y si W es un subespacio de $V(\mathscr{F})$, entonces $W_T = \{\xi T : \xi \in W\}$, la imagen de W por T, es también un subespacio de $V(\mathscr{F})$.

Para cualesquiera $\xi T, \eta T \in W_T$, tenemos $\xi T + \eta T = (\xi + \eta)T$. Como $\xi, \eta \in W$ implica $\xi + \eta \in W$, entonces es $(\xi + \eta)T \in W_T$. Así que W_T es cerrado respecto de la adición. Análogamente, para cualesquiera $\xi T \in W_T$, $s \in \mathscr{F}$ tenemos $s(\xi T) = (s\xi)T \in W_T$ puesto que $\xi \in W$ implica $s\xi \in W$. De modo que W_T es cerrado respecto de la multiplicación escalar, lo cual acaba la demostración.

18. Demostrar: El conjunto $\mathscr{A}$ de todas las transformaciones lineales de un espacio vectorial $V(\mathscr{F})$ en sí mismo, forma un anillo con respecto a la adición y multiplicación definidas por

$$A + B: \quad \xi(A + B) = \xi A + \xi B, \qquad \xi \in V(\mathscr{F})$$
$$A \cdot B: \quad \xi(A \cdot B) = (\xi A)B, \qquad \xi \in V(\mathscr{F})$$

para cualesquiera $A, B \in \mathscr{A}$.

Sea $\xi, \eta \in V(\mathscr{F})$, $k \in \mathscr{F}$ y $A, B, C \in \mathscr{A}$. Entonces,

$$(\xi + \eta)(A + B) = (\xi + \eta)A + (\xi + \eta)B = \xi A + \eta A + \xi B + \eta B$$
$$= \xi(A + B) + \eta(A + B)$$

y

$$(k\xi)(A + B) = (k\xi)A + (k\xi)B = k(\xi A) + k(\xi B)$$
$$= k(\xi A + \xi B) = k\xi(A + B)$$

Asimismo,

$$(\xi + \eta)(A \cdot B) = [(\xi + \eta)A]B = (\xi A + \eta A)B$$
$$= (\xi A)B + (\eta A)B = \xi(A \cdot B) + \eta(A \cdot B)$$

Así, pues, $A + B$, $A \cdot B \in \mathscr{A}$ y $\mathscr{A}$ es cerrado con respecto a la adición y a la multiplicación.

La adición es conmutativa y asociativa, pues

$$\xi(A + B) = \xi A + \xi B = \xi B + \xi A = \xi(B + A)$$

y

$$\begin{aligned}\xi[(A + B) + C] &= \xi(A + B) + \xi C = \xi A + \xi B + \xi C \\ &= \xi A + \xi(B + C) = \xi[A + (B + C)]\end{aligned}$$

Denótese la aplicación que aplica cada elemento de $V(\mathscr{F})$ en ζ por 0; es decir,

$$0: \quad \xi 0 = \zeta, \quad \xi \in V(\mathscr{F})$$

Entonces $0 \in \mathscr{A}$ (demuéstrese), $\xi(A + 0) = \xi A + \xi 0 = \xi A + \zeta = \xi A$

y 0 es el elemento neutro aditivo de $\mathscr{A}$.

Para todo $A \in \mathscr{A}$, sea $-A$ definido por

$$-A: \quad \xi(-A) = -(\xi A), \quad \xi \in V(\mathscr{F})$$

Se sigue fácilmente que $-A \in \mathscr{A}$ y que es el simétrico aditivo de A ya que

$$\zeta = \zeta A = (\xi - \xi)A = \xi A + [-(\xi A)] = \xi[A + (-A)] = \xi \cdot 0$$

Hemos demostrado que $\mathscr{A}$ es un grupo aditivo abeliano.

La multiplicación es asociativa desde luego, pero, en general, no es conmutativa (véase Problema 55). Para terminar la demostración de que $\mathscr{A}$ es un anillo, demostremos una de las leyes distributivas

$$A \cdot (B + C) = A \cdot B + A \cdot C$$

dejando la otra al lector. Tenemos

$$\begin{aligned}\xi[A \cdot (B + C)] &= (\xi A)(B + C) = (\xi A)B + (\xi A)C \\ &= \xi(A \cdot B) + \xi(A \cdot C) = \xi(A \cdot B + A \cdot C)\end{aligned}$$

19. Demostrar: El conjunto $\mathscr{M}$ de todas las transformaciones lineales regulares de un espacio vectorial $V(\mathscr{F})$ en sí mismo, forma un grupo multiplicativo.

Sean $A, B \in \mathscr{M}$. Como A y B son regulares, aplican $V(\mathscr{F})$ sobre $V(\mathscr{F})$, es decir, $V_A = V$ y $V_B = V$. Entonces $V_{(A \cdot B)} = (V_A)_B = V_B = V$ y $A \cdot B$ es regular. Así, pues, $A \cdot B \in \mathscr{M}$ y $\mathscr{M}$ es cerrado respecto de la multiplicación. La ley asociativa se verifica en $\mathscr{M}$ pues se verifica en $\mathscr{A}$.

Sea Z la aplicación que transforma cada elemento de $V(\mathscr{F})$ en sí mismo, es decir,

$$Z: \quad \xi Z = \xi, \quad \xi \in V(\mathscr{F})$$

Evidentemente, Z es regular, pertenece a $\mathscr{M}$ y como

$$\xi(Z \cdot A) = (\xi Z)A = \xi A = (\xi A)Z = \xi(A \cdot Z)$$

es el elemento neutro en la multiplicación.

Ahora bien, A es una aplicación biyectiva de $V(\mathscr{F})$ sobre sí mismo; de modo que tiene una inversa A^{-1} definida por

$$A^{-1}: \quad (\xi A)A^{-1} = \xi, \quad \xi \in V(\mathscr{F})$$

Para cualesquiera $\xi, \eta \in V(\mathscr{F})$, $A \in \mathscr{M}$ y $k \in \mathscr{F}$, tenemos $\xi A, \eta A \in V(\mathscr{F})$. Entonces, como

$$(\xi A + \eta A)A^{-1} = (\xi + \eta)A \cdot A^{-1} = \xi + \eta = (\xi A)A^{-1} + (\eta A)A^{-1}$$

y

$$[k(\xi A)]A^{-1} = [(k\xi)A]A^{-1} = k\xi = k[(\xi A)A^{-1}]$$

se sigue que $A^{-1} \in \mathscr{A}$. Pero, por definición, A^{-1} es regular; de manera que $A^{-1} \in \mathscr{M}$. Así, pues, todo elemento de $\mathscr{M}$ tiene un simétrico multiplicativo o inverso y $\mathscr{M}$ es un grupo multiplicativo.

Problemas propuestos

20. Utilizando la Fig. 13-1, página 143:

(*a*) Identificar los vectores (1, 0) y (0, 1); asimismo, los $(a, 0)$ y $(0, b)$.

(*b*) Comprobar que $(a, b) = (a, 0) + (0, b) = a(1, 0) + b(0, 1)$.

21. Mediante definiciones naturales de multiplicación escalar y de adición vectorial, mostrar que los siguientes son espacios vectoriales sobre el cuerpo indicado:

(*a*) $V = R$; $\mathscr{F} = Q$ (*b*) $V = C$; $\mathscr{F} = R$

(*c*) $V = \{a + b\sqrt[3]{2} + c\sqrt{3}: a, b, c \in Q\}$; $\mathscr{F} = Q$

(*d*) $V =$ todos los polinomios de grado ≤ 4 sobre R, incluido el polinomio nulo; $\mathscr{F} = Q$

(*e*) $V = \{c_1 e^x + c_2 e^{3x}: c_1, c_2 \in R\}$; $\mathscr{F} = R$

(*f*) $V = \{(a_1, a_2, a_3): a_i \in Q,\ a_1 + 2a_2 = 3a_3\}$; $\mathscr{F} = Q$

(*g*) $V = \{a + bx: a, b \in Z/(3)\}$; $\mathscr{F} = Z/(3)$

22. (*a*) ¿Por qué el conjunto de los polinomios en x de grado > 4 sobre R no es un espacio vectorial sobre R?

(*b*) ¿El conjunto de los polinomios $R[x]$ es un espacio vectorial sobre Q? ¿Y sobre C?

23. Sean $\xi, \eta \in V$ sobre $\mathscr{F}$ y $s, t \in \mathscr{F}$. Demostrar:

(*a*) Si $\xi \neq \zeta$, entonces $s\xi = t\xi$ implica $s = t$.

(*b*) Si $s \neq z$, entonces $s\xi = s\eta$ implica $\xi = \eta$.

24. Sean $\xi, \eta \neq \zeta \in V$ sobre $\mathscr{F}$. Demostrar que ξ y η son linealmente dependientes si, y solo si, $\xi = s\eta$ para algún $s \in \mathscr{F}$.

25. (*a*) Sean $\xi, \eta \in V(R)$. Si ξ y η son linealmente dependientes sobre R, ¿son linealmente dependientes sobre Q necesariamente? ¿Y sobre C?

(*b*) Considérese en (*a*) el cambio de linealmente dependiente por linealmente independiente.

26. Demostrar los Teoremas IV y VI, página 146.

27. Dado el espacio vectorial $V = V_4(R) = \{(a, b, c, d): a, b, c, d \in R\}$ sobre R, ¿cuáles de los subconjuntos que siguen son subespacios de V?

(*a*) $U = \{(a, a, a, a): a \in R\}$

(*b*) $U = \{(a, b, a, b): a, b \in Z\}$

(*c*) $U = \{(a, 2a, b, a + b): a, b \in R\}$

(*d*) $U = \{(a_1, a_2, a_3, a_4): a_i \in R,\ 2a_2 + 3a_3 = 0\}$

(*e*) $U = \{(a_1, a_2, a_3, a_4): a_i \in R,\ 2a_2 + 3a_3 = 5\}$

28. Determinar cuáles de los siguientes conjuntos de vectores de $V_3(Q)$ son linealmente dependientes o independientes sobre Q.

(*a*) $\{(0, 0, 0), (1, 1, 1)\}$ (*d*) $\{(0, 1, -2), (1, -1, 1), (1, 2, 1)\}$

(*b*) $\{(1, -2, 3), (3, -6, 9)\}$ (*e*) $\{(0, 2, -4), (1, -2, -1), (1, -4, 3)\}$

(*c*) $\{(1, -2, -3), (3, 2, 1)\}$ (*f*) $\{(1, -1, -1), (2, 3, 1), (-1, 4, -2), (3, 10, 8)\}$

Resp. (*c*), (*d*) son linealmente independientes.

29. Determinar si los siguientes conjuntos de vectores de $V_3(Z/(5))$ son linealmente dependientes o independientes sobre $Z/(5)$.

(*a*) $\{(1, 2, 4), (2, 4, 1)\}$ (*c*) $\{(0, 1, 1), (1, 0, 1), (3, 3, 2)\}$

(*b*) $\{(2, 3, 4), (3, 2, 1)\}$ (*d*) $\{(4, 1, 3), (2, 3, 1), (4, 1, 0)\}$

Resp. (*a*), (*c*) son linealmente independientes.

30. Dado el conjunto $S = \{(1, 2, 1), (2, 3, 2), (3, 2, 3), (1, 1, 1)\}$ de vectores de $V(Z/(5))$ hallar un conjunto máximo linealmente independiente T y expresar cada uno de los restantes vectores como combinación lineal de los elementos de T.

31. Hallar la dimensión del subconjunto de $V_3(Q)$ generado por cada uno de los conjuntos de vectores del Problema 28.
Resp. (*a*), (*b*) 1; (*c*), (*e*) 2; (*d*), (*f*) 3

32. Para el espacio vectorial C sobre R, demostrar
(*a*) $\{1, i\}$ es una base
(*b*) $\{a + bi, c + di\}$ es una base si, y solo si, $ad - bc \neq 0$.

33. En cada uno de los siguientes casos, hallar una base del espacio vectorial que incluya los vectores indicados:
(*a*) $\{(1, 1, 0), (0, 1, 1)\}$ en $V_3(Q)$.
(*b*) $\{(2, 1, -1, -2), (2, 3, -2, 1), (4, 2, -1, 3)\}$ en $V_4(Q)$.
(*c*) $\{(2, 1, 1, 0), (1, 2, 0, 1)\}$ en $V_4(Z/(3))$.
(*d*) $\{(i, 0, 1, 0), (0, i, 1, 0)\}$ en $V_4(C)$.

34. Demostrar que $S = \{\xi_1, \xi_2, \xi_3\} = \{i, 1 + i, 2\}, (2 + i, i, 1), (3, 3 + 2i, -1)\}$ es una base de $V_3(C)$ y expresar los vectores unitarios de $V_3(C)$ como combinaciones lineales de los elementos de S.

Resp. $e_1 = [(-39 - 6i)\xi_1 + (80 - i)\xi_2 + (2 - 13i)\xi_3]/173$
$e_2 = [(86 - 40i)\xi_1 + (-101 + 51i)\xi_2 + (71 - 29i)\xi_3]/346$
$e_3 = [(104 + 16i)\xi_1 + (75 - 55i)\xi_2 + (-63 - 23i)\xi_3]/346$

35. Demostrar: Si $k_1\xi_1 + k_2\xi_2 + k_3\xi_3 = \zeta$ con $k_1k_2 \neq z$, entonces $\{\xi_1, \xi_3\}$ y $\{\xi_2, \xi_3\}$ generan el mismo espacio.

36. Demostrar el Teorema IX, página 147.

37. Demostrar: Si $\{\xi_1, \xi_2, \xi_3\}$ es una base de $V_3(Q)$, también lo es $\{\xi_1 + \xi_2, \xi_2 + \xi_3, \xi_3 + \xi_1\}$. ¿Es esto cierto en $V_3(Z/(2))$? ¿En $V_3(Z/(3))$?

38. Demostrar el Teorema X, página 147. *Sugerencia*: Supóngase que A y B, de m y n elementos, respectivamente, son bases de V. Primero asóciese S con A y T con B, luego S con B y T con A y aplíquese el Teorema VIII, página 147.

39. Demostrar: Si V es un espacio vectorial de dimensión $n \geq 0$, cualquier conjunto linealmente independiente de n vectores de V es una base.

40. Sean $\xi_1, \xi_2, \ldots, \xi_m \in V$ y $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ que genera un subespacio $U \subset V$. Demostrar que el mínimo de vectores de V necesarios para generar U es el máximo de vectores linealmente independientes de S.

41. Sea $\{\xi_1, \xi_2, \ldots, \xi_n\}$ una base de V. Demostrar que todo vector $\xi \in V$ tiene una representación única como combinación lineal de los vectores de base.
Sugerencia. Supóngase $\xi = \sum c_i\xi_i = \sum d_i\xi_i$; entonces $\sum c_i\xi_i - \sum d_i\xi_i = \xi$.

42. Demostrar: Si U y W son subespacios de un espacio vectorial V, también lo son $U \cap W$ y $U + W$.

43. Sean los subespacios U y W de $V_4(Q)$ generados por

$$A = \{(2, -1, 1, 0), (1, 0, 2, 1)\} \quad \text{y} \quad B = \{(0, 0, 1, 0), (0, 1, 0, 1), (4, -1, 5, 2)\}$$

respectivamente. Comprobar el Teorema XIII, página 148. Encontrar una base de $U + W$ que incluya los vectores de A; también una base que incluya los vectores de B.

44. Demostrar que $P = \{(a, b, -b, a)\colon a, b \in R\}$ con adición definida por

$$(a, b, -b, a) + (c, d, -d, c) = \big(a + c, b + d, -(b + d), a + c\big)$$

y multiplicación escalar definida por $k(a, b, -b, a) = (ka, kb, -kb, ka)$ para todo $(a, b, -b, a), (c, d, -d, c) \in P$ y $k \in R$, es un espacio vectorial de dimensión dos.

45. Sea el primo p un elemento primo de G del Problema 8, Capítulo 10. Denótese por $\mathscr{F}$ el cuerpo $G/(p)$ y por $\mathscr{F}'$ el cuerpo primo $Z/(p)$ de $\mathscr{F}$. El cuerpo $\mathscr{F}$, considerado como espacio vectorial sobre $\mathscr{F}'$, tiene por base $\{1, i\}$: luego $\mathscr{F} = \{a_1 \cdot 1 + a_2 \cdot i\colon a_1, a_2 \in \mathscr{F}'\}$. (*a*) Demostrar que $\mathscr{F}$ tiene a lo más p^2 elementos. (*b*) Demostrar que $\mathscr{F}$ tiene al menos p^2 elementos (esto es, $a_1 \cdot 1 + a_2 \cdot i = b_1 \cdot 1 + b_2 \cdot i$ si, y solo si, $a_1 - b_1 = a_2 - b_2 = 0$) y que, por tanto, tiene exactamente p^2 elementos.

46. Generalizar el Problema 45 a un cuerpo finito $\mathscr{F}$ de característica prima p, sobre su cuerpo primo con n elementos como base.

47. Para $\xi, \eta, \mu \in V_n(R)$ y $k \in R$ demostrar

(*a*) $\xi \cdot \eta = \eta \cdot \xi$. (*b*) $(\xi + \eta) \cdot \mu = \xi \cdot \mu + \eta \cdot \mu$, (*c*) $(k\xi \cdot \eta) = k(\xi \cdot \eta)$.

48. De la desigualdad de Schwarz obtener $-1 \leq (\xi \cdot \eta)/(|\xi| \cdot |\eta|) \leq 1$ para demostrar que $\cos\theta = \dfrac{\xi \cdot \eta}{|\xi| \cdot |\eta|}$ determina un ángulo único entre 0° y 180°.

49. Supóngase la longitud definida como en $V_n(R)$. Demuéstrese que $(1, 1) \in V_2(Q)$ carece de longitud en tanto que $(1, i) \in V_2(C)$ es de longitud 0. ¿Es posible dar una definición de $\xi \cdot \eta$ tal que todo vector no nulo de $V_2(C)$ tenga longitud diferente de 0?

50. Sean $\xi, \eta \in V_n(R)$ tales que $|\xi| = |\eta|$. Demostrar que $\xi - \eta$ y $\xi + \eta$ son ortogonales. ¿Cuál es la interpretación geométrica?

51. Para el espacio vectorial V de todos los polinomios en x sobre un cuerpo $\mathscr{F}$, comprobar que las siguientes aplicaciones de V en sí mismo son transformaciones lineales de V.

(*a*) $a(x) \to a(x)$ (*c*) $a(x) \to a(-x)$

(*b*) $a(x) \to -a(x)$ (*d*) $a(x) \to a(0)$

52. Demostrar que la aplicación T: $(a, b) \to (a + 1, b + 1)$ de $V_2(R)$ en sí mismo no es una transformación lineal. *Sugerencia.* Compárese $(\epsilon_1 + \epsilon_2)T$ con $(\epsilon_1 T + \epsilon_2 T)$.

53. Para cada una de las transformaciones lineales A, estudiar la imagen de un vector arbitrario ξ para determinar la característica de A y, si A es singular, determinar un vector no nulo cuya imagen sea 0.

(*a*) A: $\epsilon_1 \to (2, 1)$, $\epsilon_2 \to (1, 2)$

(*b*) A: $\epsilon_1 \to (3, -4)$, $\epsilon_2 \to (-3, 4)$

(*c*) A: $\epsilon_1 \to (1, 1, 2)$, $\epsilon_2 \to (2, 1, 3)$, $\epsilon_3 \to (1, 0, -2)$

(*d*) A: $\epsilon_1 \to (1, -1, 1)$, $\epsilon_2 \to (-3, 3, -3)$, $\epsilon_3 \to (2, 3, 4)$

(*e*) A: $\epsilon_1 \to (0, 1, -1)$, $\epsilon_2 \to (-1, 1, 1)$, $\epsilon_3 \to (1, 0, -2)$

(*f*) A: $\epsilon_1 \to (1, 0, 3)$, $\epsilon_2 \to (0, 1, 1)$, $\epsilon_3 \to (2, 2, 8)$

Resp. (*a*) regular; (*b*) singular, $(1, 1)$; (*c*) regular; (*d*) singular, $(3, 1, 0)$; (*e*) singular, $(-1, 1, 1)$; (*f*) singular, $(2, 2, -1)$.

54. Para cualesquiera $A, B \in \mathscr{A}$ y $k, l \in \mathscr{F}$ demostrar

(*a*) $kA \in \mathscr{A}$

(*b*) $k(A + B) = kA + kB$; $(k + l)A = kA + lA$

(*c*) $k(A \cdot B) = (kA)B = A(kB)$; $(k \cdot l)A = k(lA)$

(*d*) $0 \cdot A = k0 = 0$; $uA = A$

con 0 definido en la página 159. Junto con el Ejercicio 18, esto completa la demostración del Teorema XX, página 152.

55. Calcular $B \cdot A$ de las transformaciones lineales del Ejemplo 13, página 152, para demostrar que, en general, $A \cdot B \neq B \cdot A$.

56. Para las transformaciones lineales sobre $V_3(R)$

$$A: \begin{cases} \epsilon_1 \to (a, b, c) \\ \epsilon_2 \to (d, e, f) \\ \epsilon_3 \to (g, h, i) \end{cases} \quad \text{y} \quad B: \begin{cases} \epsilon_1 \to (j, k, l) \\ \epsilon_2 \to (m, n, p) \\ \epsilon_3 \to (q, r, s) \end{cases}$$

obtener

$$A + B: \begin{cases} \epsilon_1 \to (a + j, b + k, c + l) \\ \epsilon_2 \to (d + m, e + n, f + p) \\ \epsilon_3 \to (g + q, h + r, i + s) \end{cases}$$

$$A \cdot B: \begin{cases} \epsilon_1 \to (aj+bm+cq, ak+bn+cr, al+bp+cs) \\ \epsilon_2 \to (dj+em+fq, dk+en+fr, dl+ep+fs) \\ \epsilon_3 \to (gj+hm+iq, gk+hn+ir, gl+hp+is) \end{cases}$$

y, para todo $k \in R$,

$$kA: \begin{cases} \epsilon_1 \to (ka, kb, kc) \\ \epsilon_2 \to (kd, ke, kf) \\ \epsilon_3 \to (kg, kh, ki) \end{cases}$$

57. Calcular la inversa A^{-1} de $A: \begin{cases} \epsilon_1 \to (1,1) \\ \epsilon_2 \to (2,3) \end{cases}$ de $V_2(R)$.

Sugerencia: Tómese $A^{-1}: \begin{cases} \epsilon_1 \to (p,q) \\ \epsilon_2 \to (r,s) \end{cases}$ y considérese $(\xi A)A^{-1} = \xi$ donde $\xi = (a, b)$.

Resp. $\begin{cases} \epsilon_1 \to (3,-1) \\ \epsilon_2 \to (-2,1) \end{cases}$

58. Para la aplicación

$$T_1: \begin{cases} \epsilon_1 = (1,0) \to (1,1,1) \\ \epsilon_2 = (0,1) \to (0,1,2) \end{cases} \qquad \text{de } V = V_2(R) \text{ en } W = V_3(R)$$

verificar que:

(*a*) T_1 es una transformación lineal de V en W.

(*b*) La imagen de $\xi = (2,1) \in V$ es $(2,3,4) \in W$.

(*c*) El vector $(1,2,2) \in W$ no es imagen.

(*d*) V_{T_1} tiene dimensión 2.

59. Para la aplicación

$$T_2: \begin{cases} \epsilon_1 = (1,0,0) \to (1,0,1,1) \\ \epsilon_2 = (0,1,0) \to (0,1,1,1) \\ \epsilon_3 = (0,0,1) \to (1,-1,0,0) \end{cases} \qquad \text{de } V = V_3(R) \text{ en } W = V_4(R)$$

comprobar que:

(*a*) T_2 es una transformación lineal de V en W.

(*b*) La imagen de $\xi = (1,-1,-1) \in V$ es $(0,0,0,0) \in W$.

(*c*) V_{T_2} tiene dimensión 2 y $r_{T_2} = 2$.

60. Para T_1 del Problema 58 y T_2 del Problema 59, verificar que

$$T_1 \cdot T_2: \begin{cases} \epsilon_1 = (1,0) \to (2,0,2,2) \\ \epsilon_2 = (0,1) \to (2,-1,1,1) \end{cases}$$

¿Cuál es la característica de $T_1 \cdot T_2$?

Capítulo 14

Matrices

INTRODUCCION

Considérense de nuevo las transformaciones lineales sobre $V_3(R)$

$$A: \begin{cases} \epsilon_1 \to (a, b, c) \\ \epsilon_2 \to (d, e, f) \\ \epsilon_3 \to (g, h, i) \end{cases} \quad \text{y} \quad B: \begin{cases} \epsilon_1 \to (j, k, l) \\ \epsilon_2 \to (m, n, p) \\ \epsilon_3 \to (q, r, s) \end{cases} \tag{1}$$

para las cuales (véase Problema 56, Capítulo 13, página 162)

$$A + B: \begin{cases} \epsilon_1 \to (a + j, b + k, c + l) \\ \epsilon_2 \to (d + m, e + n, f + p) \\ \epsilon_3 \to (g + q, h + r, i + s) \end{cases}$$

$$A \cdot B: \begin{cases} \epsilon_1 \to (aj + bm + cq, ak + bn + cr, al + bp + cs) \\ \epsilon_2 \to (dj + em + fq, dk + en + fr, dl + ep + fs) \\ \epsilon_3 \to (gj + hm + iq, gk + hn + ir, gl + hp + is) \end{cases}$$

$$kA: \begin{cases} \epsilon_1 \to (ka, kb, kc) \\ \epsilon_2 \to (kd, ke, kf) \\ \epsilon_3 \to (kg, kh, ki) \end{cases}, \quad k \in R$$

Con el objeto de simplificar, remplácese esta notación de las transformaciones lineales A y B por los cuadros

$$A = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} j & k & l \\ m & n & p \\ q & r & s \end{bmatrix} \tag{2}$$

que se obtienen poniendo los vectores imagen entre corchetes y eliminando paréntesis y comas sobrantes. El problema que se nos presenta es traducir las operaciones con transformaciones lineales a operaciones correspondientes con estos cuadros. Así tenemos:

La *suma* $A + B$ de los cuadros A y B es el cuadro cuyos elementos son las sumas de los elementos correspondientes de A y B.

El *producto escalar* kA de un escalar cualquiera k por A es el cuadro cuyos elementos son k veces los correspondientes elementos del A.

Al formar el producto $A \cdot B$ piénsese que A consiste en los vectores ρ_1, ρ_2, ρ_3 (los *vectores fila* de A), cuyos componentes son los elementos de las filas de A y que B consiste en los vectores γ_1, γ_2, γ_3 (los *vectores columna* de B), cuyos componentes son los elementos de las columnas de B. Entonces,

$$A \cdot B = \begin{bmatrix} \rho_1 \\ \rho_2 \\ \rho_3 \end{bmatrix} \cdot [\gamma_1 \ \gamma_2 \ \gamma_3] = \begin{bmatrix} \rho_1 \cdot \gamma_1 & \rho_1 \cdot \gamma_2 & \rho_1 \cdot \gamma_3 \\ \rho_2 \cdot \gamma_1 & \rho_2 \cdot \gamma_2 & \rho_2 \cdot \gamma_3 \\ \rho_3 \cdot \gamma_1 & \rho_3 \cdot \gamma_2 & \rho_3 \cdot \gamma_3 \end{bmatrix}$$

donde $\rho_i \cdot \gamma_j$ es el producto interno de ρ_i y γ_j. Nótese cuidadosamente que en $A \cdot B$ aparece el producto interno de cada vector fila de A por cada vector columna de B; así como también que los elementos de cualquier fila de $A \cdot B$ son los productos internos, cuyo primer factor es el vector fila correspondiente de A.

Ejemplo 1:

(*a*) Si $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ y $B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$ sobre Q, se tiene

$$A + B = \begin{bmatrix} 1+5 & 2+6 \\ 3+7 & 4+8 \end{bmatrix} = \begin{bmatrix} 6 & 8 \\ 10 & 12 \end{bmatrix}, \qquad 10A = \begin{bmatrix} 10 \cdot 1 & 10 \cdot 2 \\ 10 \cdot 3 & 10 \cdot 4 \end{bmatrix} = \begin{bmatrix} 10 & 20 \\ 30 & 40 \end{bmatrix}$$

$$A \cdot B = \left[\begin{array}{cc} 1 & 2 \\ \hline 3 & 4 \end{array}\right] \cdot \left[\begin{array}{c|c} 5 & 6 \\ 7 & 8 \end{array}\right] = \begin{bmatrix} 1 \cdot 5 + 2 \cdot 7 & 1 \cdot 6 + 2 \cdot 8 \\ 3 \cdot 5 + 4 \cdot 7 & 3 \cdot 6 + 4 \cdot 8 \end{bmatrix} = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix}$$

y $$B \cdot A = \left[\begin{array}{cc} 5 & 6 \\ \hline 7 & 8 \end{array}\right] \cdot \left[\begin{array}{c|c} 1 & 2 \\ 3 & 4 \end{array}\right] = \begin{bmatrix} 5+18 & 10+24 \\ 7+24 & 14+32 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ 31 & 46 \end{bmatrix}$$

(*b*) Si $A = \begin{bmatrix} 1 & 0 & -2 \\ 0 & -3 & 1 \\ 2 & 1 & 0 \end{bmatrix}$ y $B = \begin{bmatrix} 3 & -1 & 0 \\ -2 & 0 & 3 \\ 0 & 2 & -1 \end{bmatrix}$ sobre Q, se tiene

$$A \cdot B = \begin{bmatrix} 3 & -1-4 & 2 \\ 6 & 2 & -9-1 \\ 6-2 & -2 & 3 \end{bmatrix} = \begin{bmatrix} 3 & -5 & 2 \\ 6 & 2 & -10 \\ 4 & -2 & 3 \end{bmatrix} \quad \text{y} \quad B \cdot A = \begin{bmatrix} 3 & 3 & -7 \\ 4 & 3 & 4 \\ -2 & -7 & 2 \end{bmatrix}$$

MATRICES CUADRADAS

Los cuadros de la sección precedente, con los cuales se ha definido una adición, una multiplicación y una multiplicación escalar, se llaman matrices cuadradas; más exactamente, son *matrices cuadradas de orden* 3, pues tienen 3^2 elementos. (En el Ejemplo 1(*a*) las matrices cuadradas son de orden 2.)

Para poder escribir completamente matrices cuadradas de órdenes mayores vamos a introducir una notación más uniforme. En lo que sigue, los elementos de una matriz cuadrada se denotarán por una sola letra afectada de subíndices que varían, por ejemplo:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \quad \text{y} \quad B = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{bmatrix}$$

Cualquier elemento, como el b_{24}, por ejemplo, se ha de considerar como $b_{2,4}$, si bien, al menos que sea necesario (como en b_{121}, que podría ser $b_{12,1}$ o $b_{1,21}$), no se pondrá la coma. Una ventaja de esta notación es que cada elemento indica su posición en la matriz. Por ejemplo, el elemento b_{24} está en la segunda fila y cuarta columna, el b_{32} en la tercera fila y segunda columna, etc. Otra ventaja es que podemos indicar las matrices A y B anteriores con solo escribir

$$A = [a_{ij}], \quad (i = 1,2,3;\ j = 1,2,3)$$

y

$$B = [b_{ij}], \quad (i = 1,2,3,4;\ j = 1,2,3,4)$$

Entonces, para la A definida y $C = [c_{ij}]$, $(i, j = 1, 2, 3)$, el producto es

$$A \cdot C = \begin{bmatrix} \sum a_{1j}c_{j1} & \sum a_{1j}c_{j2} & \sum a_{1j}c_{j3} \\ \sum a_{2j}c_{j1} & \sum a_{2j}c_{j2} & \sum a_{2j}c_{j3} \\ \sum a_{3j}c_{j1} & \sum a_{3j}c_{j2} & \sum a_{3j}c_{j3} \end{bmatrix}$$

donde en cada casilla la sumación se extiende a todos los valores de j; por ejemplo,

$$\sum a_{2j}c_{j3} = a_{21}c_{13} + a_{22}c_{23} + a_{23}c_{33}, \text{ etc.}$$

Dos matrices cuadradas L y M se dirán iguales, $L = M$, si, y solo si, una es duplicado de la otra, esto es, si, y solo si, L y M son la misma transformación lineal. De modo que dos matrices iguales tienen necesariamente el mismo orden.

En una matriz cuadrada se llama *diagonal principal* la diagonal que va de la esquina superior izquierda a la inferior derecha. Los elementos de la diagonal principal son los que tienen igual índice de fila y de columna y solamente ellos (por ejemplo, a_{11}, a_{22}, a_{33} de A).

Por definición, hay una aplicación biyectiva entre el conjunto de todas las transformaciones lineales de un espacio vectorial sobre $\mathscr{F}$ de dimensión n en sí mismo y el conjunto de todas las matrices cuadradas sobre $\mathscr{F}$ de orden n (el conjunto de todas las matrices cuadradas de orden n sobre $\mathscr{F}$). Además, hemos definido con estas matrices una adición y una multiplicación, de tal modo que esta aplicación es un isomorfismo. De modo que por los Teoremas XVIII y XIX del Capítulo 13, página 152, tenemos

Teorema I. El conjunto de las matrices cuadradas de orden n sobre $\mathscr{F}$ dotado de adición y multiplicación, es un anillo unitario $\mathscr{R}$.

En consecuencia:

La adición es asociativa y conmutativa sobre $\mathscr{R}$.

La multiplicación es asociativa, pero, en general, no es conmutativa sobre $\mathscr{R}$.

La multiplicación es distributiva a izquierda y a derecha con respecto a la adición.

Existe una matriz nula, 0_n ó 0, elemento cero de $\mathscr{R}$, cada uno de cuyos elementos es el cero de $\mathscr{F}$.

Por ejemplo, $0_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ y $0_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ son *matrices nulas* sobre R de órdenes 2 y 3, respectivamente.

Existe una matriz I_n o I, la unidad de $\mathscr{R}$, que tiene por elementos de la diagonal principal la unidad de $\mathscr{F}$ y en todos los otros lugares tiene por elementos el cero de $\mathscr{F}$. Por ejemplo, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ e $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ son *matrices unidad* sobre R de órdenes 2 y 3, respectivamente.

Para toda $A = [a_{ij}] \in \mathscr{R}$ existe una simétrica aditiva $-A = (-1)[a_{ij}] = [-a_{ij}]$ tal que $A + (-A) = 0$.

En lo que queda del libro utilizaremos 0 y 1, respectivamente, para denotar el elemento cero y el elemento unidad de todo cuerpo (página 118). Siempre que aparezcan z y u, originalmente reservados para denotar estos elementos, tendrán connotaciones diferentes. Así, pues, se usarán 0 e I como se acaban de definir sobre R para las matrices nula y unidad sobre cualquier cuerpo $\mathscr{F}$.

Por el Teorema XX, Capítulo 13, página 152, tenemos

Teorema II. El conjunto de las matrices cuadradas de orden n sobre $\mathscr{F}$ es un espacio vectorial.

Un conjunto de elementos de base para este espacio vectorial consiste en las n^2 matrices

$$E_{ij},\ (i, j = 1, 2, 3, \ldots, n)$$

de orden n que tienen 1 como elemento en el lugar (i, j) y 0 en todos los otros. Por ejemplo,

$$\{E_{11}, E_{12}, E_{21}, E_{22}\} = \left\{\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}, \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}\right\}$$

es una base del espacio vectorial de las matrices cuadradas de orden 2 sobre $\mathscr{F}$; y para toda matriz $A = \begin{bmatrix}a & b\\ c & d\end{bmatrix}$, tenemos $A = aE_{11} + bE_{12} + cE_{21} + dE_{22}$.

ALGEBRA MATRICIAL TOTAL

El conjunto de todas las matrices cuadradas de orden n sobre $\mathscr{F}$ con las operaciones de adición, multiplicación y multiplicación escalar por elementos de $\mathscr{F}$ se llama *álgebra matricial total* $\mathscr{M}_n(\mathscr{F})$. Ahora bien, así como hay subgrupos de grupos, subanillos de anillos, ..., asimismo hay subálgebras de $\mathscr{M}_n(\mathscr{F})$. Por ejemplo, el conjunto de todas las matrices $\mathscr{M}$ de la forma $\begin{bmatrix}a & b & c\\ 2c & a & b\\ 2b & 2c & a\end{bmatrix}$, donde $a, b, c \in Q$ es una subálgebra de $\mathscr{M}_3(Q)$. Todo lo que hay que demostrar es que la adición, la multiplicación y la multiplicación escalar por elementos de Q sobre elementos de $\mathscr{M}$ producen elementos de $\mathscr{M}$. La adición y la multiplicación escalar no presentan dificultad, y así $\mathscr{M}$ es un subespacio del espacio vectorial $\mathscr{M}_3(Q)$. En cuanto a la multiplicación, nótese que una base de $\mathscr{M}$ es el conjunto

$$\left\{I,\ X = \begin{bmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 2 & 0 & 0\end{bmatrix},\ Y = \begin{bmatrix}0 & 0 & 1\\ 2 & 0 & 0\\ 0 & 2 & 0\end{bmatrix}\right\}.$$ Dejamos al lector el demostrar que para $A, B \in \mathscr{M}$,

$$\begin{aligned} A \cdot B &= (aI + bX + cY)(xI + yX + zY)\\ &= (ax + 2bz + 2cy)I + (ay + bx + 2cz)X + (az + by + cx)Y \in \mathscr{M}; \end{aligned}$$

así que la multiplicación es conmutativa sobre $\mathscr{M}$.

MATRIZ DE ORDEN $m \times n$

Por matriz sobre $\mathscr{F}$ se entiende toda disposición rectangular de elementos de $\mathscr{F}$; por ejemplo,

$$A = \begin{bmatrix}a_{11} & a_{12} & a_{13}\\ a_{21} & a_{22} & a_{23}\\ a_{31} & a_{32} & a_{33}\end{bmatrix}, \qquad B = \begin{bmatrix}b_{11} & b_{12} & b_{13} & b_{14}\\ b_{21} & b_{22} & b_{23} & b_{24}\\ b_{31} & b_{32} & b_{33} & b_{34}\end{bmatrix}, \qquad C = \begin{bmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\\ c_{31} & c_{32}\\ c_{41} & c_{42}\end{bmatrix}$$

o bien $A = [a_{ij}],\ (i, j = 1, 2, 3) \qquad B = [b_{ij}],\ (i = 1, 2, 3;\ j = 1, 2, 3, 4)$

$$C = [c_{ij}],\ (i = 1, 2, 3, 4;\ j = 1, 2)$$

Una matriz semejante de m filas y n columnas se dirá *matriz de orden* $m \times n$.

Para m y n dados, considérese el conjunto de las matrices sobre $\mathscr{F}$ de orden $m \times n$. Con la adición y multiplicación escalar definidas exactamente como para las matrices cuadradas, tenemos el

Teorema II. El conjunto de las matrices sobre $\mathscr{F}$ de orden $m \times n$ es un espacio vectorial sobre $\mathscr{F}$.

No puede definirse la multiplicación sobre este conjunto al menos que $m = n$. No obstante, podemos definir, como en el Problema 60, Capítulo 13, página 163, se sugiere, el producto de *ciertos* cuadros rectangulares. Por ejemplo, utilizando las matrices A, B, C anteriores, podemos formar $A \cdot B$, pero no $B \cdot A$; $B \cdot C$, pero no $C \cdot B$; ni tampoco $A \cdot C$ ni $C \cdot A$. La razón es clara: para formar $L \cdot M$, el número de columnas de L debe ser igual al número de filas de M. Para las B y C dadas, tenemos

$$B \cdot C = \begin{bmatrix} \rho_1 \\ \rho_2 \\ \rho_3 \end{bmatrix} \cdot [\gamma_1 \ \gamma_2] = \begin{bmatrix} \rho_1 \cdot \gamma_1 & \rho_1 \cdot \gamma_2 \\ \rho_2 \cdot \gamma_1 & \rho_2 \cdot \gamma_2 \\ \rho_3 \cdot \gamma_1 & \rho_3 \cdot \gamma_2 \end{bmatrix} = \begin{bmatrix} \sum b_{1j} c_{j1} & \sum b_{1j} c_{j2} \\ \sum b_{2j} c_{j1} & \sum b_{2j} c_{j2} \\ \sum b_{3j} c_{j1} & \sum b_{3j} c_{j2} \end{bmatrix}$$

Así, pues, el producto de una matriz de orden $m \times n$ por una matriz de orden $n \times p$, ambas sobre el mismo cuerpo $\mathscr{F}$, es una matriz de orden $m \times p$.

Véanse Problemas 2-3.

SOLUCIONES DE UN SISTEMA DE ECUACIONES LINEALES

Hasta ahora el estudio de las matrices ha estado presidido por nuestro estudio previo de las transformaciones lineales de espacios vectoriales. Podríamos, sin embargo, haber comenzado el estudio de las matrices observando la aplicación biyectiva entre todos los sistemas de ecuaciones lineales homogéneas sobre R y el conjunto de los cuadros de sus coeficientes; por ejemplo,

$$\left.\begin{array}{ll} \text{(i)} & 2x + 3y + z = 0 \\ \text{(ii)} & x - y + 4z = 0 \\ \text{(iii)} & 4x + 11y - 5z = 0 \end{array}\right\} \quad \text{y} \quad \begin{bmatrix} 2 & 3 & 1 \\ 1 & -1 & 4 \\ 4 & 11 & -5 \end{bmatrix} \tag{3}$$

Lo que vamos a hacer aquí es demostrar que una matriz, considerada como matriz coeficiente de un sistema de ecuaciones homogéneas, puede utilizarse (en lugar de las ecuaciones mismas) para obtener soluciones del sistema. En lo que sigue expresamos nuestros «pasos», el resultado de nuestros «pasos», con las ecuaciones, y, por último, en forma de matriz.

El sistema (*3*) dado tiene la solución trivial $x = y = z = 0$; tiene soluciones no triviales si, y solo si, una de las ecuaciones es una combinación lineal de las otras dos, es decir, si, y solo si, los vectores fila de la matriz de coeficientes son linealmente dependientes. El procedimiento para encontrar soluciones no triviales, si las hay, es bien conocido. El conjunto de «pasos» no es único; procederemos como sigue: multiplicamos la segunda ecuación por 2 y la restamos de la primera; luego multiplicamos la segunda ecuación por 4 y la restamos de la tercera, obteniendo así

$$\begin{array}{ll} \text{(i)} - 2\text{(ii)} & 0x + 5y - 7z = 0 \\ \text{(ii)} & x - y + 4z = 0 \\ \text{(lll)} - 4\text{(ii)} & 0x + 15y - 21z = 0 \end{array} \qquad \begin{bmatrix} 0 & 5 & -7 \\ 1 & -1 & 4 \\ 0 & 15 & -21 \end{bmatrix} \tag{4}$$

En (*4*), multiplicamos la primera ecuación por 3 y la restamos de la tercera:

$$\begin{array}{ll} \text{(i)} - 2\text{(ii)} & 0x + 5y - 7z = 0 \\ \text{(ii)} & x - y + 4z = 0 \\ \text{(iii)} + 2\text{(ii)} - 3\text{(i)} & 0x + 0y + 0z = 0 \end{array} \qquad \begin{bmatrix} 0 & 5 & -7 \\ 1 & -1 & 4 \\ 0 & 0 & 0 \end{bmatrix} \tag{5}$$

Por último, en (*5*), multiplicamos la primera ecuación por 1/5 y, poniéndola de primera ecuación en (*6*), la sumamos a la segunda. Tenemos

$$\begin{array}{ll} \frac{1}{5}[\text{(i)} - 2\text{(ii)}] & 0x + y - 7z/5 = 0 \\ \frac{1}{5}[3\text{(ii)} + \text{(i)}] & x + 0y + 13z/5 = 0 \\ \text{(iii)} + 2\text{(ii)} - 3\text{(i)} & 0x + 0y + 0z = 0 \end{array} \qquad \begin{bmatrix} 0 & 1 & -7/5 \\ 1 & 0 & 13/5 \\ 0 & 0 & 0 \end{bmatrix} \tag{6}$$

Si ahora tomamos para z cualquier $r \in R$ arbitrario, tenemos como solución del sistema: $x = -13r/5$, $y = 7r/5$, $z = r$.

Resumiendo: del sistema de ecuaciones dado (3) sacamos la matriz $A = \begin{bmatrix} 2 & 3 & 1 \\ 1 & -1 & 4 \\ 4 & 11 & -5 \end{bmatrix}$; operando sobre las filas de A llegamos a la matriz $B = \begin{bmatrix} 0 & 1 & -7/5 \\ 1 & 0 & 13/5 \\ 0 & 0 & 0 \end{bmatrix}$; considerando B como una matriz coeficiente en las mismas incógnitas, leemos la solución del sistema original. Damos ahora tres problemas de espacios vectoriales cuyas soluciones se siguen fácilmente:

Ejemplo 2: ¿Es $\xi_1 = (2, 1, 4)$, $\xi_2 = (3, -1, 11)$, $\xi_3 = (1, 4, -5)$ una base de $V_3(R)$?

Hacemos $x\xi_1 + y\xi_2 + z\xi_3 = (2x + 3y + z, x - y + 4z, 4x + 11y - 5z) = 0 = (0, 0, 0)$ y obtenemos el sistema de ecuaciones (3). Mediante la solución $x = -13/5$, $y = 7/5$, $z = 1$, encontramos que $\xi_3 = (13/5)\xi_1 - (7/5)\xi_2$. Así que el conjunto dado no es una base, lo cual naturalmente está implicado por la matriz (5) que tiene una fila de ceros.

Ejemplo 3: ¿El conjunto $\rho_1 = (2, 3, 1)$, $\rho_2 = (1, -1, 4)$, $\rho_3 = (4, 11, -5)$ es una base de $V_3(R)$?

Los vectores dados son los vectores fila de (3). De los pasos indicados en (5) se deduce (iii) + 2(ii) − 3(i) = 0, o sea $\rho_3 + 2\rho_2 - 3\rho_1 = 0$. Así que el conjunto dicho no es una base.

Nota. Los problemas resueltos en los Ejemplos 2 y 3 son del mismo tipo y los cálculos son idénticos; los procedimientos iniciales, sin embargo, son bien diferentes. En el Ejemplo 2 los vectores dados constituyen las columnas de la matriz y las operaciones con la matriz implican combinaciones lineales de las componentes correspondientes de estos vectores. En el Ejemplo 3 los vectores dados constituyen las filas de la matriz y las operaciones con esta matriz implican combinaciones lineales de los vectores mismos. Seguiremos utilizando la notación del Capítulo 13, en que un vector de $V_n(\mathscr{F})$ se escribe como una fila de elementos y así utilizaremos de ahora en adelante el procedimiento del Ejemplo 3.

Ejemplo 4: Demostrar que la transformación lineal

$$T: \begin{cases} \epsilon_1 \to (2, 3, 1) = \rho_1 \\ \epsilon_2 \to (1, -1, 4) = \rho_2 \\ \epsilon_3 \to (4, 11, -5) = \rho_3 \end{cases}$$

de $V = V_3(R)$ es singular y hallar un vector de V cuya imagen sea 0.

Se escribe $T = \begin{bmatrix} 2 & 3 & 1 \\ 1 & -1 & 4 \\ 4 & 11 & -5 \end{bmatrix} = \begin{bmatrix} \rho_1 \\ \rho_2 \\ \rho_3 \end{bmatrix}$. Por el Ejemplo 3, $\rho_3 + 2\rho_2 - 3\rho_1 = 0$; de modo que la imagen de cualquier vector de V es una combinación lineal de los vectores ρ_1 y ρ_2. Luego V_T tiene dimensión 2 y T es singular, cosa que, desde luego, implica la matriz (5), que tiene una sola fila de ceros.

Como $3\rho_1 - 2\rho_2 - \rho_3 = 0$, la imagen de $\eta = (3, -2, -1)$ es 0, esto es,

$$(3, -2, -1) \cdot \begin{bmatrix} 2 & 3 & 1 \\ 1 & -1 & 4 \\ 4 & 11 & -5 \end{bmatrix} = 0$$

Nota. El vector $(3, -2, -1)$ puede considerarse como una matriz 1×3; con lo que el producto indicado es válido.

Véase Problema 4.

TRANSFORMACIONES ELEMENTALES DE UNA MATRIZ

Al resolver un sistema de ecuaciones lineales homogéneas con coeficientes en $\mathscr{F}$ se pueden realizar ciertas operaciones con los elementos (ecuaciones) del sistema sin que cambie su solución o soluciones:

Se pueden permutar dos ecuaciones cualesquiera.
Toda ecuación se puede multiplicar por un escalar cualquiera $k \neq 0$ de $\mathscr{F}$.

Se puede multiplicar cualquier ecuación por cualquier escalar y sumarla a cualquier otra ecuación.

Las operaciones que esto induce sobre la matriz coeficiente del sistema son las llamadas *transformaciones elementales de fila* siguientes:

La permutación de las filas i y j denotada por H_{ij}.
La multiplicación de cada elemento de la fila i por un escalar no nulo k y denotada por $H_i(k)$.
La adición de los elementos de la fila i de k (un escalar) veces los correspondientes elementos de la fila j, cosa que se denota por $H_{ij}(k)$.

Después veremos la utilidad de las *transformaciones elementales de columna* sobre una matriz que enumeramos ahora:

La permutación de las columnas i y j denotada por K_{ij}.
La multiplicación de cada elemento de la columna i por un escalar no nulo k, denotada por $K_i(k)$.
La adición a los elementos de la columna i de k (un escalar) veces los elementos correspondientes de la columna j, lo cual se denota por $K_{ij}(k)$.

Dos matrices A y B se dirán *equivalentes por fila* (*columna*) si B puede obtenerse de A mediante una sucesión de transformaciones elementales de *fila* (*columna*). De igual modo se dirá que dos matrices A y B son *equivalentes* si B puede obtenerse de A mediante una sucesión de transformaciones de fila y columna. Si B es equivalente por fila, por columna, o equivalente a A, escribiremos $B \sim A$. Dejamos al lector la demostración de que $\sim$ es una relación de equivalencia.

Ejemplo 5: (*a*) Demostrar que el conjunto $\{(1, 2, 1, 2), (2, 4, 3, 4), (1, 3, 2, 3), (0, 3, 1, 3)\}$ no es una base de $V_4(Q)$. (*b*) Si T es la transformación lineal que tiene los vectores de (*a*) por imágenes, en su orden, de ϵ_1, ϵ_2, ϵ_3, ϵ_4, ¿cuál es la característica de T? (*c*) Hallar una base de $V_4(Q)$ que contenga un subconjunto máximo linealmente independiente de vectores de (*a*).

(*a*) Utilizando sucesivamente $H_{21}(-2)$, $H_{31}(-1)$; $H_{13}(-2)$, $H_{43}(-3)$; $H_{42}(2)$, tenemos

$$A = \begin{bmatrix} 1 & 2 & 1 & 2 \\ 2 & 4 & 3 & 4 \\ 1 & 3 & 2 & 3 \\ 0 & 3 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 3 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & -2 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

El conjunto no es una base.

(*b*) Utilizando $H_{12}(1)$, $H_{32}(-1)$ en la matriz final obtenida en (*a*), tenemos

$$A \sim \begin{bmatrix} 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} = B$$

Y B tiene el número máximo de ceros posible en una matriz equivalente por fila a A (comprobarlo). Como B tiene 3 vectores fila no nulos, V_T es de dimensión 3 y $r_T = 3$.

(*c*) Revisando los pasos dados, se ve que no se ha agregado un múltiplo de la cuarta fila a ninguna de las otras tres. Así que los tres primeros vectores del conjunto dado son combinaciones lineales de los vectores fila no nulos de B. Los primeros tres vectores del conjunto dado junto con cualquier vector que no sea combinación lineal de los vectores fila no nulos de B, como ϵ_2 o ϵ_4, por ejemplo, forman una base de $V_4(Q)$.

Considerando las filas de una matriz dada A como un conjunto S de vectores fila de $V_n(\mathscr{F})$, interprétense las transformaciones elementales de fila sobre A en términos de los vectores de S como:

Permutación de dos vectores cualesquiera de S.

Sustitución de cualquier vector $\xi \in S$ por un múltiplo escalar no nulo $a\xi$.

Sustitución de cualquier vector $\xi \in S$ por una combinación lineal $\xi + b\eta$ de ξ y cualquier otro vector $\eta \in S$.

Los ejemplos anteriores ilustran el

Teorema III. Las operaciones que preceden efectuadas en un conjunto S de vectores de $V_n(\mathscr{F})$ no aumentan ni disminuyen el número de vectores linealmente independientes de S.

Véanse Problemas 5-7.

MATRICES TRIANGULARES SUPERIORES, TRIANGULARES INFERIORES Y DIAGONALES

Una matriz cuadrada $A = [a_{ij}]$ se dice *triangular superior* si $a_{ij} = 0$ para $i > j$, y se dice *triangular inferior* si $a_{ij} = 0$ para $i < j$. Una matriz cuadrada que es simultáneamente triangular superior e inferior se llama matriz *diagonal*. Por ejemplo, $\begin{bmatrix} 1 & 2 & 3 \\ 0 & 0 & 4 \\ 0 & 0 & 2 \end{bmatrix}$ es triangular superior, $\begin{bmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 3 & 4 & 5 \end{bmatrix}$ es triangular inferior, pero $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 2 \end{bmatrix}$ y $\begin{bmatrix} -2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ son diagonales.

Mediante transformaciones elementales, toda matriz cuadrada puede reducirse a una triangular superior, triangular inferior y diagonal.

Ejemplo 6:

Reducir $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 8 \end{bmatrix}$ sobre Q a triangular superior, triangular inferior y diagonal.

(a) Con $H_{21}(-4)$, $H_{31}(-5)$; $H_{32}(-1)$, obtenemos

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 8 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -3 & -7 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & -1 \end{bmatrix}$$ que es triangular superior.

(b) Con $H_{12}(-2/5)$, $H_{23}(-5/7)$; $H_{12}(-21/10)$, $H_{23}(-1/28)$

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 8 \end{bmatrix} \sim \begin{bmatrix} -3/5 & 0 & 3/5 \\ 3/7 & 0 & 2/7 \\ 5 & 7 & 8 \end{bmatrix} \sim \begin{bmatrix} -3/2 & 0 & 0 \\ 1/4 & -1/4 & 0 \\ 5 & 7 & 8 \end{bmatrix}$$ que es triangular inferior.

(c) Con $H_{21}(-4)$, $H_{31}(-5)$, $H_{32}(-1)$; $H_{12}(2/3)$, $H_{13}(-1)$, $H_{23}(-6)$

$$A \sim \begin{bmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & -1 \\ 0 & -3 & -6 \\ 0 & 0 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$ que es diagonal.

Véase también Problema 8.

UNA FORMA CANONICA

En el Ejercicio 9 demostramos el

Teorema IV. Toda matriz no nula A sobre $\mathscr{F}$ puede reducirse por sucesivas transformaciones elementales de fila a una *matriz canónica por filas* (*matriz escalón*) C que tiene las propiedades siguientes:

(i) Cada una de las primeras r filas de C tiene al menos un elemento no nulo; las filas restantes, si las hay, consisten en elementos ceros únicamente.

(ii) En la fila i ($i = 1, 2, \ldots, r$) de C, el primer elemento no nulo es 1. Numérese j_i la columna en que está este elemento.

(iii) El único elemento no nulo en la columna numerada j_i ($i = 1, 2, \ldots, r$) es el elemento 1 de la fila i.

(iv) $j_1 < j_2 < \cdots < j_r$.

Ejemplo 7: (*a*) La matriz B del Problema 6, página 187, es una matriz canónica por filas. El primer elemento no nulo de la primera fila es 1 y se encuentra en la primera columna, el primer elemento no nulo de la segunda fila es 1 y se encuentra en la segunda columna, el primer elemento no nulo de la tercera fila es 1 y se encuentra en la quinta columna. Así, pues, $j_1 = 1$, $j_2 = 2$, $j_3 = 5$ y se cumple $j_1 < j_2 < j_3$.

(*b*) La matriz B del Problema 7, página 187, no cumple la condición (iv) y no es, por tanto, una matriz canónica por filas. Pero se la puede reducir a

$$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = C,$$

que es una matriz canónica por filas, mediante las transformaciones elementales de fila H_{12}, H_{13}.

En el Problema 5, página 186, la matriz B es una matriz canónica por filas; es también la matriz unidad de orden 3. La transformación lineal A es regular y así también llamaremos regular la matriz A. Así, pues,

Una matriz cuadrada de orden n es *regular* si, y solo si, es equivalente por fila a la matriz unidad I_n.

Toda matriz cuadrada de orden n no regular se dirá *singular*. Los términos singular y regular jamás se emplean si la matriz es de orden $m \times n$ con $m \neq n$.

La característica de una transformación lineal A es el número de vectores linealmente independientes en el conjunto de vectores imagen. La característica de la transformación lineal A la llamaremos característica de fila de la matriz A. Así que

La *característica de fila* de una matriz $m \times n$ es el número de filas no nulas en su matriz canónica por filas equivalente.

Desde luego no se precisa reducir una matriz a forma canónica por filas para determinar su característica. Por ejemplo, la característica de la matriz A del Problema 7 se puede obtener tan fácilmente de B como de la matriz canónica por filas C del Ejemplo 7(*b*).

TRANSFORMACIONES ELEMENTALES DE COLUMNA

Partiendo de una matriz A y utilizando solamente transformaciones elementales de columna, podemos obtener matrices llamadas equivalentes por columna de A. Entre éstas hay una *matriz canónica por columnas* D cuyas propiedades son precisamente las obtenidas al intercambiar «fila» y «columna» en las propiedades enumeradas para la matriz canónica por filas C. Se define como *característica de columna* de A el número de columnas de D que tienen al menos un elemento distinto de cero. Lo único que aquí nos interesa es el

Teorema V. La característica de fila y la característica de columna de toda matriz A son iguales.

Para una demostración, véase el Problema 10.

Como consecuencia, definimos

La *característica* de una matriz es su característica de fila (columna).

Sea una matriz A sobre $\mathscr{F}$ de orden $m \times n$ y característica r reducida a su forma canónica por filas C. Entonces, utilizando el elemento 1 que aparece en cada una de las primeras r filas de C y mediante transformaciones apropiadas del tipo $K_{ij}(k)$, C puede reducirse a una matriz cuyos únicos ele-

mentos distintos de cero son estos 1. Por último, por transformaciones del tipo K_{ij}, estos 1 se pueden llevar a ocupar las posiciones diagonales en las primeras r filas y r columnas. La matriz que resulta, denotada por N, se llama *forma normal* de A.

Ejemplo 8:

(*a*) En el Problema 4 tenemos

$$A = \begin{bmatrix} 1 & 2 & 2 & 0 \\ 2 & 5 & 3 & 1 \\ 3 & 8 & 4 & 2 \\ 2 & 7 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 4 & -2 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = C$$

Usando $K_{31}(-4), K_{41}(2)$; $K_{32}(1), K_{42}(-1)$ sobre C, obtenemos

$$A \sim \begin{bmatrix} 1 & 0 & 4 & -2 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} I_2 & 0 \\ 0 & 0 \end{bmatrix}, \text{ la forma normal}$$

(*b*) La matriz B es la forma normal de A en el Problema 5.

(*c*) Para la matriz del Problema 6 obtenemos, mediante las transformaciones elementales de columna aplicadas a B, $K_{31}(-4), K_{32}(1), K_{42}(-2)$; K_{35}

$$A \sim \begin{bmatrix} 1 & 0 & 4 & 0 & 0 \\ 0 & 1 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = [I_3 \ 0]$$

Nota. Por estos ejemplos se podría pensar que al reducir A a su forma normal hay que aplicar primero transformaciones de fila y luego exclusivamente transformaciones de columna. Pero este orden no es necesario.

Véase Problema 11.

MATRICES ELEMENTALES

La matriz que resulta de aplicar una transformación elemental de fila (columna) a la matriz unidad I_n se llama *matriz fila (columna) elemental*. Toda matriz fila (columna) elemental se denotará por el mismo símbolo que se emplea para denotar la transformación elemental que produce la matriz.

Ejemplo 9:

Si es $I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, tenemos

$$H_{13} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = K_{13}, \quad H_2(k) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & 1 \end{bmatrix} = K_2(k), \quad H_{23}(k) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & k \\ 0 & 0 & 1 \end{bmatrix} = K_{32}(k)$$

Por el Teorema III tenemos

Teorema VI. Toda matriz elemental es regular.

y

Teorema VII. El producto de dos o más matrices elementales es regular.

De aquí se deduce fácilmente

Teorema VIII. Para hacer una transformación elemental de fila (columna) H (K) sobre una matriz A de orden $m \times n$, hágase el producto $H \cdot A$ ($A \cdot K$) donde H (K) es la matriz que se obtiene por la transformación H (K) sobre I.

Las matrices H y K del Teorema VIII no llevan indicación de su orden. Si A es de orden $m \times n$, un producto tal como el $H_{13} \cdot A \cdot K_{23}(k)$ ha de implicar que H_{13} es de orden m en tanto que $K_{23}(k)$ es de orden n, ya que de otra manera el producto indicado no tendría sentido.

Ejemplo 10: Dada $A = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 \end{bmatrix}$ sobre Q, calcular

$$(a)\quad H_{13} \cdot A = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 6 & 8 \\ 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 \end{bmatrix}$$

$$(b)\quad H_1(-3) \cdot A = \begin{bmatrix} -3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 \end{bmatrix} = \begin{bmatrix} -3 & -6 & -9 & -12 \\ 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 \end{bmatrix}$$

$$(c)\quad A \cdot K_{41}(-4) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 2 & 4 & 6 & 8 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & -4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 0 \\ 5 & 6 & 7 & -12 \\ 2 & 4 & 6 & 0 \end{bmatrix}$$

Supóngase ahora que $H_1, H_2, \ldots, H_s$ y $K_1, K_2, \ldots, K_t$ son sucesiones de transformaciones elementales que, realizadas en el orden de sus subíndices sobre una matriz A, la reducen a B, es decir,

$$H_s \cdot \ldots \cdot H_2 \cdot H_1 \cdot A \cdot K_1 \cdot K_2 \cdot \ldots \cdot K_t = B$$

Entonces, definiendo $S = H_s \cdot \ldots \cdot H_2 \cdot H_1$ y $T = K_1 \cdot K_2 \cdot \ldots \cdot K_t$ tenemos

$$S \cdot A \cdot T = B$$

Con lo que A y B son matrices equivalentes. La demostración del recíproco

Teorema IX. Si A y B son matrices equivalentes, existen matrices regulares S y T tales que $S \cdot A \cdot T = B$.

se dará en la sección siguiente.

Como consecuencia del Teorema IX, tenemos

Teorema IX'. Para toda matriz A existen matrices regulares S y T tales que $S \cdot A \cdot T = N$, la forma normal de A.

Ejemplo 11: Hallar matrices regulares S y T sobre Q tales que

$$S \cdot A \cdot T = S \cdot \begin{bmatrix} 1 & 2 & -1 \\ 3 & 8 & 2 \\ 4 & 9 & -1 \end{bmatrix} \cdot T = N, \quad \text{la forma normal de } A.$$

Con $H_{21}(-3), H_{31}(-4), K_{21}(-2), K_{31}(1)$, hallamos $A = \begin{bmatrix} 1 & 2 & -1 \\ 3 & 8 & 2 \\ 4 & 9 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 5 \\ 0 & 1 & 3 \end{bmatrix}$. Entonces, con $H_{23}(-1)$, obtenemos $A \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 3 \end{bmatrix}$ y, por último, $H_{32}(-1)$, $K_{32}(-2)$ dan la forma normal $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. Así, pues,

$$H_{32}(-1) \cdot H_{23}(-1) \cdot H_{31}(-4) \cdot H_{21}(-3) \cdot A \cdot K_{21}(-2) \cdot K_{31}(1) \cdot K_{32}(-2)$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -4 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot A \cdot \begin{bmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & -1 \\ -5 & -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & -1 \\ 3 & 8 & 2 \\ 4 & 9 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

He aquí otro procedimiento: empezamos con el cuadro

$$\begin{array}{cccccccc} & & & & 1 & 0 & 0 & \\ & & & & 0 & 1 & 0 & \\ & & & & 0 & 0 & 1 & \\ & & & & 1 & 2 & -1 & 1 & 0 & 0 \\ & & I_3 & & 3 & 8 & 2 & 0 & 1 & 0 \\ A & I_3 & = & & 4 & 9 & -1 & 0 & 0 & 1 \end{array}$$

y procedemos a reducir A a I. Al hacer esto, cada transformación de fila se aplica a las filas de seis elementos y cada transformación de columna se aplica a las columnas de seis elementos. Mediante $H_{21}(-3)$, $H_{31}(-4)$; $K_{21}(-2)$, $K_{31}(1)$; $H_{23}(-1)$; $H_{32}(-1)$; $K_{32}(-2)$ obtenemos

$$\begin{array}{cccccc} 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ 1 & 2 & -1 & 1 & 0 & 0 \\ 3 & 8 & 2 & 0 & 1 & 0 \\ 4 & 9 & -1 & 0 & 0 & 1 \end{array} \rightarrow \begin{array}{cccccc} 1 & 0 & 0 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ 1 & 2 & -1 & 1 & 0 & 0 \\ 0 & 2 & 5 & -3 & 1 & 0 \\ 0 & 1 & 8 & -4 & 0 & 1 \end{array} \rightarrow \begin{array}{cccccc} 1 & -2 & 1 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 5 & -3 & 1 & 0 \\ 0 & 1 & 3 & -4 & 0 & 1 \end{array}$$

$$\begin{array}{cccccc} 1 & -2 & 1 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 & -1 \\ 0 & 1 & 3 & -4 & 0 & 1 \end{array} \rightarrow \begin{array}{cccccc} 1 & -2 & 1 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 & -1 \\ 0 & 0 & 1 & -5 & -1 & 2 \end{array} \rightarrow \begin{array}{cccccc} 1 & -2 & 5 & & & \\ 0 & 1 & -2 & & & \\ 0 & 0 & 1 & & & \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & -1 \\ 0 & 0 & 1 & -5 & -1 & 2 \end{array} \quad \begin{matrix} & \\ & \\ & \\ & \\ & T \\ = & I \end{matrix} \quad S$$

y $S \cdot A \cdot T = I$, como antes.

Véase también Problema 12.

INVERSAS DE MATRICES ELEMENTALES

Para cada una de las transformaciones elementales hay una transformación inversa, es decir, una transformación que deshace lo hecho por la transformación elemental. Expresadas por transformaciones elementales o por matrices elementales, hallamos

$$H_{ij}^{-1} = H_{ij} \qquad K_{ij}^{-1} = K_{ij}$$

$$H_i^{-1}(k) = H_i(1/k) \qquad K_i^{-1}(k) = K_i(1/k)$$

$$H_{ij}^{-1}(k) = H_{ij}(-k) \qquad K_{ij}^{-1}(k) = K_{ij}(-k)$$

Así, pues,

Teorema X. La inversa de una transformación elemental de fila (columna) es una transformación elemental de fila (columna) de igual orden.

y

Teorema XI. La inversa de una matriz fila (columna) elemental es regular.

En el Ejercicio 13 demostramos

Teorema XII. La inversa del producto de dos matrices A y B, cada una de las cuales tiene inversa, es el producto de las inversas en orden inverso, es decir,

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$$

El Teorema XII se puede generalizar de inmediato a la inversa del producto de cualquier número de matrices. En particular tenemos:

$$\text{si } S = H_s \cdot \ldots \cdot H_2 \cdot H_1 \quad \text{es} \quad S^{-1} = H_1^{-1} \cdot H_2^{-1} \cdot \ldots \cdot H_s^{-1},$$

$$\text{si } T = K_1 \cdot K_2 \cdot \ldots \cdot K_t \quad \text{es} \quad T^{-1} = K_t^{-1} \cdot \ldots \cdot K_2^{-1} \cdot K_1^{-1}.$$

Supóngase A de orden $m \times n$. Por el Teorema IX' existen matrices regulares S de orden m y T de orden n tales que $S \cdot A \cdot T = N$, la forma normal de A. Entonces,

$$A = S^{-1}(S \cdot A \cdot T)T^{-1} = S^{-1} \cdot N \cdot T^{-1}$$

En particular tenemos

Teorema XIII. Si A es regular y si $S \cdot A \cdot T = I$, entonces

$$A = S^{-1} \cdot T^{-1}$$

esto es, toda matriz regular de orden n se puede expresar como producto de matrices elementales del mismo orden.

Ejemplo 12: En el ejemplo 11 tenemos

$$S = H_{32}(-1) \cdot H_{23}(-1) \cdot H_{31}(-4) \cdot H_{21}(-3) \quad \text{y} \quad T = K_{21}(-2) \cdot K_{31}(1) \cdot K_{32}(-2)$$

Entonces,

$$S^{-1} = H_{21}^{-1}(-3) \cdot H_{31}^{-1}(-4) \cdot H_{23}^{-1}(-1) \cdot H_{32}^{-1}(-1) = H_{21}(3) \cdot H_{31}(4) \cdot H_{23}(1) \cdot H_{32}(1)$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & 1 \\ 4 & 1 & 1 \end{bmatrix},$$

$$T^{-1} = K_{32}(2) \cdot K_{31}(-1) \cdot K_{21}(2) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix}$$

y $$A = S^{-1} \cdot T^{-1} = \begin{bmatrix} 1 & 0 & 0 \\ 3 & 2 & 1 \\ 4 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & -1 \\ 3 & 8 & 2 \\ 4 & 9 & -1 \end{bmatrix}.$$

Supóngase que A y B sobre $\mathscr{F}$ de orden $m \times n$ tienen la misma característica. Tienen entonces la misma forma normal N y existen matrices regulares S_1, T_1; S_2, T_2 tales que $S_1AT_1 = N = S_2BT_2$. Mediante las inversas S_1^{-1} y T_1^{-1} de S_1 y T_1 obtenemos

$$A = S_1^{-1} \cdot S_1AT_1 \cdot T_1^{-1} = S_1^{-1} \cdot S_2BT_2 \cdot T_1^{-1} = (S_1^{-1} \cdot S_2)B(T_2 \cdot T_1^{-1}) = S \cdot B \cdot T$$

Así que A y B son equivalentes. Dejamos la recíproca al lector y enunciamos el

Teorema XIV. Dos matrices A y B sobre $\mathscr{F}$ de orden $m \times n$ son equivalentes si, y solo si, tienen la misma característica.

INVERSA DE UNA MATRIZ REGULAR

La inversa A^{-1}, si existe, de una matriz cuadrada A tiene la propiedad

$$A \cdot A^{-1} = A^{-1} \cdot A = I$$

Como la característica de un producto de dos matrices no puede exceder la característica de ninguno de los factores (véase Capítulo 13), tenemos

Teorema XV. La inversa de una matriz A existe si, y solo si, A es regular.

Sea A regular. Por el Teorema IX' existen matrices regulares S y T tales que $S \cdot A \cdot T = I$. Entonces, $A = S^{-1} \cdot T^{-1}$, y por el Teorema XII,

$$A^{-1} = (S^{-1} \cdot T^{-1})^{-1} = T \cdot S$$

Ejemplo 13:

Mediante los resultados del Ejemplo **11**, hallamos que

$$A^{-1} = T \cdot S = \begin{bmatrix} 1 & -2 & 5 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & -1 \\ -5 & -1 & 2 \end{bmatrix} = \begin{bmatrix} -26 & -7 & 12 \\ 11 & 3 & -5 \\ -5 & -1 & 2 \end{bmatrix}$$

Al calcular la inversa de una matriz regular, es más simple utilizar solamente transformaciones elementales de fila.

Ejemplo 14:

Hallar la inversa de $A = \begin{bmatrix} 1 & 2 & -1 \\ 3 & 8 & 2 \\ 4 & 9 & -1 \end{bmatrix}$ del Ejemplo **11** utilizando solamente transformaciones elementales de fila.

Tenemos

$$[A \;\; I] = \left[\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0 \\ 3 & 8 & 2 & 0 & 1 & 0 \\ 4 & 9 & -1 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0 \\ 0 & 2 & 5 & -3 & 1 & 0 \\ 0 & 1 & 3 & -4 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 2 & -1 & 1 & 0 & 0 \\ 0 & 1 & 3 & -4 & 0 & 1 \\ 0 & 2 & 5 & -3 & 1 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 0 & -7 & 9 & 0 & -2 \\ 0 & 1 & 3 & -4 & 0 & 1 \\ 0 & 0 & -1 & 5 & 1 & -2 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & -26 & -7 & 12 \\ 0 & 1 & 0 & 11 & 3 & -5 \\ 0 & 0 & 1 & -5 & -1 & 2 \end{array}\right] = [I \;\; A^{-1}].$$

Véase también Problema 14.

POLINOMIO MINIMO DE UNA MATRIZ CUADRADA

Sea $A \neq 0$ una matriz de orden n sobre $\mathscr{F}$. Como $A \in \mathscr{M}_n(\mathscr{F})$, el conjunto $\{I, A, A^2, \ldots, A^{n^2}\}$ es linealmente dependiente y existen escalares $a_0, a_1, a_2, \ldots, a_{n^2}$ no todos nulos tales que

$$\phi(A) = a_0 I + a_1 A + a_2 A^2 + \cdots + a_{n^2} A^{n^2} = 0$$

En esta sección nos ocuparemos del polinomio mónico $m(\lambda) \in \mathscr{F}[\lambda]$ de grado mínimo tal que $m(A) = 0$. Es claro que o bien $m(\lambda) = \phi(\lambda)$ o bien $m(\lambda)$ es un divisor propio de $\phi(\lambda)$. En uno u otro caso $m(\lambda)$ se dirá *polinomio mínimo* de A.

El procedimiento más elemental de obtener el polinomio mínimo de $A \neq 0$ es el siguiente:

(1) Si $A = a_0 I$, $a_0 \in \mathscr{F}$, entonces $m(\lambda) = \lambda - a_0$.

(2) Si $A \neq aI$, para todo $a \in \mathscr{F}$, pero $A^2 = a_1 A + a_0 I$ con $a_0, a_1 \in \mathscr{F}$, entonces $m(\lambda) = \lambda^2 - a_1\lambda - a_0$.

(3) Si $A^2 \neq aA + bI$ para todo $a, b \in \mathscr{F}$, pero $A^3 = a_2 A^2 + a_1 A + a_0 I$ con $a_0, a_1, a_2 \in \mathscr{F}$, entonces $m(\lambda) = \lambda^3 - a_2\lambda^2 - a_1\lambda - a_0$.

y así sucesivamente.

Ejemplo 15:

Hallar el polinomio mínimo de $A = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$ sobre Q.

Como $A \neq a_0 I$ para todo $a_0 \in Q$,

$$A^2 = \begin{bmatrix} 9 & 8 & 8 \\ 8 & 9 & 8 \\ 8 & 8 & 9 \end{bmatrix} = a_1 \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix} + a_0 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 + a_0 & 2a_1 & 2a_1 \\ 2a_1 & a_1 + a_0 & 2a_1 \\ 2a_1 & 2a_1 & a_1 + a_0 \end{bmatrix}$$

Después de verificar cada término, concluimos que $A^2 = 4A + 5I$ y el polinomio mínimo es $\lambda^2 - 4\lambda - 5$.

Véase también Problema 15.

El Ejemplo 15 y el Problema 15 sugieren que el término constante del polinomio mínimo de $A \neq 0$ es distinto de cero si, y solo si, A es regular. Un segundo procedimiento para calcular la inversa de una matriz regular se desprende entonces de aquí.

Ejemplo 16: Hallar la inversa A^{-1}, sabiendo que el polinomio mínimo de $A = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 1 \end{bmatrix}$ (véase Ejemplo 15) es $\lambda^2 - 4\lambda - 5$.

Como $A^2 - 4A - 5I = 0$, tenemos, tras multiplicar por A^{-1}, $A - 4I - 5A^{-1} = 0$;

$$\text{luego} \quad A^{-1} = \tfrac{1}{5}(A - 4I) = \begin{bmatrix} -3/5 & 2/5 & 2/5 \\ 2/5 & -3/5 & 2/5 \\ 2/5 & 2/5 & -3/5 \end{bmatrix}.$$

SISTEMAS DE ECUACIONES LINEALES

Sean $\mathscr{F}$ un cuerpo dado y las indeterminadas $x_1, x_2, \ldots, x_n$. Por *forma lineal* sobre $\mathscr{F}$ en las n indeterminadas, se entiende un polinomio del tipo

$$ax_1 + bx_2 + \cdots + px_n$$

en que $a, b, \ldots, p \in \mathscr{F}$. Considérese ahora un sistema de m ecuaciones lineales

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = h_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = h_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = h_m \end{cases} \tag{7}$$

en el que tanto los coeficientes a_{ij} como los términos constantes h_i son elementos de $\mathscr{F}$. Es de notar que el signo de igualdad en (7) no se puede interpretar como en los capítulos anteriores, ya que en cada ecuación el segundo miembro está en $\mathscr{F}$, pero el primero no. Siguiendo la práctica corriente, escribimos (7) para indicar que se buscan elementos $r_1, r_2, \ldots, r_n \in \mathscr{F}$ tales que al remplazar los x_i por los r_i $(i = 1, 2, \ldots, n)$ el sistema se compondrá de igualdades entre elementos de $\mathscr{F}$. Un conjunto semejante de elementos r_i se dice *solución* de (7).

Denótese por $\qquad A = [a_{ij}], \quad (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n)$

la matriz coeficiente de (7) y por $S = \{\xi_1, \xi_2, \ldots, \xi_m\}$ el conjunto de vectores fila de A. Como los ξ_i son vectores de $V_n(\mathscr{F})$, el número de vectores linealmente independientes en S es $r \leq n$. Sin perder generalidad, podemos (y así lo haremos) suponer que estos r vectores linealmente independientes constituyen las primeras r filas de A, lo cual, en efecto, lo más que exige es escribir las ecuaciones de (7) en orden diferente.

Supóngase ahora que hemos hallado un vector $\rho = (r_1, r_2, \ldots, r_n) \in V_n(\mathscr{F})$ tal que

$$\xi_1 \cdot \rho = h_1, \quad \xi_2 \cdot \rho = h_2, \quad \ldots, \quad \xi_r \cdot \rho = h_r$$

Como cada ξ_i $(i = r + 1, r + 2, \ldots, m)$ es combinación lineal con coeficientes en $\mathscr{F}$ de los r vectores linealmente independientes de A, se sigue que

$$\xi_{r+1} \cdot \rho = h_{r+1}, \quad \xi_{r+2} \cdot \rho = h_{r+2}, \quad \ldots, \quad \xi_m \cdot \rho = h_m \tag{8}$$

y $x_1 = r_1, x_2 = r_2, \ldots, x_n = r_n$ es una solución de (7) si, y solo si, en (8) cada h_i es la misma combinación lineal de $h_1, h_2, \ldots, h_r$ que es ξ_i del conjunto $\xi_1, \xi_2, \ldots, \xi_r$, es decir, si, y solamente si, la característica de fila de la *matriz aumentada* $[A \ \ H] = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} & h_1 \\ a_{21} & a_{22} & \ldots & a_{2n} & h_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & h_m \end{bmatrix}$ es también r.

Hemos demostrado así el

Teorema XVI. Un sistema (7) de m ecuaciones lineales en n incógnitas tiene solución si, y solo si, la característica de fila de la matriz coeficiente A y la de la matriz aumentada $[A\ H]$ del sistema son iguales.

Supóngase que A y $[A\ H]$ tienen igual característica de fila $r < n$ y que $[A\ H]$ se ha reducido a su forma canónica de fila

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 & c_{1,r+1} & c_{1,r+2} & \dots & c_{1n} & k_1 \\ 0 & 1 & 0 & \dots & 0 & c_{2,r+1} & c_{2,r+2} & \dots & c_{2n} & k_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & c_{r,r+1} & c_{r,r+2} & \dots & c_{rn} & k_r \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 \end{bmatrix}.$$

Dense valores arbitrarios $s_{r+1}, s_{r+2}, \dots, s_n \in \mathscr{F}$ a $x_{r+1}, x_{r+2}, \dots, x_n$; entonces,

$$\begin{aligned} x_1 &= k_1 - c_{1,r+1} \cdot s_{r+1} - c_{1,r+2} \cdot s_{r+2} - \cdots - c_{1n} \cdot s_n \\ x_2 &= k_2 - c_{2,r+1} \cdot s_{r+1} - c_{2,r+2} \cdot s_{r+2} - \cdots - c_{2n} \cdot s_n \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ x_r &= k_r - c_{r,r+1} \cdot s_{r+1} - c_{r,r+2} \cdot s_{r+2} - \cdots - c_{rn} \cdot s_n \end{aligned}$$

quedan univocamente determinadas. Tenemos

Teorema XVI'. En un sistema (7) en el cual la característica común de fila de A y $[A\ H]$ es $r < n$, se pueden dar valores arbitrarios en $\mathscr{F}$ a $n - r$ incógnitas y entonces las restantes r incógnitas quedan unívocamente determinadas en función de éstas.

Sistemas de ecuaciones lineales no homogéneas.

El sistema (7) se llama de ecuaciones lineales no homogéneas sobre $\mathscr{F}$ si no todos los $h_i = 0$. Para saber si un tal sistema tiene o no una solución y cómo se halla la solución (soluciones), si existe, procedemos a reducir la matriz aumentada $[A\ H]$ del sistema a su forma canónica de fila. Las distintas posibilidades se ilustran en los ejemplos que siguen.

Ejemplo 17:

Considérese el sistema $\begin{cases} x_1 + 2x_2 - 3x_3 + x_4 = 1 \\ 2x_1 - x_2 + 2x_3 - x_4 = 1 \\ 4x_1 + 3x_2 - 4x_3 + x_4 = 2 \end{cases}$ sobre Q.

Tenemos

$$[A\ H] = \begin{bmatrix} 1 & 2 & -3 & 1 & 1 \\ 2 & -1 & 2 & -1 & 1 \\ 4 & 3 & -4 & 1 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 1 \\ 0 & -5 & 8 & -3 & -1 \\ 0 & -5 & 8 & -3 & -2 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -3 & 1 & 1 \\ 0 & -5 & 8 & -3 & -1 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

Si bien ésta no es la forma canónica de fila, vemos, en seguida, que

$$r_A = 2 < 3 = r_{[A\ H]}$$

y el sistema es *incompatible*, es decir, carece de solución.

Ejemplo 18:

Considérese el sistema $\begin{cases} x_1 + 2x_2 - x_3 = -1 \\ 3x_1 + 8x_2 + 2x_3 = 28 \\ 4x_1 + 9x_2 - x_3 = 14 \end{cases}$ sobre Q.

Tenemos

$$[A\ \ H] = \begin{bmatrix} 1 & 2 & -1 & -1 \\ 3 & 8 & 2 & 28 \\ 4 & 9 & -1 & 14 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -1 & -1 \\ 0 & 2 & 5 & 31 \\ 0 & 1 & 3 & 18 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & -1 & -1 \\ 0 & 1 & 3 & 18 \\ 0 & 2 & 5 & 31 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & -7 & -37 \\ 0 & 1 & 3 & 18 \\ 0 & 0 & -1 & -5 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & -2 \\ 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 5 \end{bmatrix}.$$

Aquí, $r_A = r_{[A\ H]} = 3$ = número de incógnitas. Hay una única solución: $x_1 = -2$, $x_2 = 3$, $x_3 = 5$.

Ejemplo 19:

Considérese el sistema $\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 3 \\ 2x_1 + 3x_2 + 3x_3 + x_4 - x_5 = 0 \\ -x_1 + 2x_2 - 5x_3 + 2x_4 - x_5 = 1 \\ 3x_1 - x_2 + 2x_3 - 3x_4 - 2x_5 = -1 \end{cases}$ sobre Q.

Tenemos

$$[A\ \ H] = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 3 \\ 2 & 3 & 3 & 1 & -1 & 0 \\ -1 & 2 & -5 & 2 & -1 & 1 \\ 3 & -1 & 2 & -3 & -2 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 3 \\ 0 & 1 & 1 & -1 & -3 & -6 \\ 0 & 3 & -4 & 3 & 0 & 4 \\ 0 & -4 & -1 & -6 & -5 & -10 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 2 & 4 & 9 \\ 0 & 1 & 1 & -1 & -3 & -6 \\ 0 & 0 & -7 & 6 & 9 & 22 \\ 0 & 0 & 3 & -10 & -17 & -34 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 2 & 4 & 9 \\ 0 & 1 & 1 & -1 & -3 & -6 \\ 0 & 0 & -1 & -14 & -25 & -46 \\ 0 & 0 & 3 & -10 & -17 & -34 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 2 & 4 & 9 \\ 0 & 1 & 1 & -1 & -3 & -6 \\ 0 & 0 & 1 & 14 & 25 & 46 \\ 0 & 0 & 3 & -10 & -17 & -34 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 2 & 4 & 9 \\ 0 & 1 & 0 & -15 & -28 & -52 \\ 0 & 0 & 1 & 14 & 25 & 46 \\ 0 & 0 & 0 & -52 & -92 & -172 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 2 & 4 & 9 \\ 0 & 1 & 0 & -15 & -28 & -52 \\ 0 & 0 & 1 & 14 & 25 & 46 \\ 0 & 0 & 0 & 1 & 23/13 & 43/13 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 6/13 & 31/13 \\ 0 & 1 & 0 & 0 & -19/13 & -31/13 \\ 0 & 0 & 1 & 0 & 3/13 & -4/13 \\ 0 & 0 & 0 & 1 & 23/13 & 43/13 \end{bmatrix}$$

Aquí A y $[A\ H]$ tienen ambas característica 4; el sistema es *compatible*, es decir, tiene una o más soluciones. A diferencia del sistema del Ejemplo 18, la característica es menor que el número de incógnitas. Ahora bien,

el sistema dado es equivalente a $\begin{cases} x_1 + \frac{6}{13}x_5 = 31/13 \\ x_2 - \frac{19}{13}x_5 = -31/13 \\ x_3 + \frac{3}{13}x_5 = -4/13 \\ x_4 + \frac{23}{13}x_5 = 43/13 \end{cases}$ y es claro que si damos a x_5 cualquier valor

$r \in Q$, entonces $x_1 = (31 - 6r)/13$, $x_2 = (-31 + 19r)/13$, $x_3 = (-4 - 3r)/13$, $x_4 = (43 - 23r)/13$, $x_5 = r$ es una solución. Por ejemplo, $x_1 = 1$, $x_2 = 2$, $x_3 = -1$, $x_4 = -2$, $x_5 = 3$ y $x_1 = 31/13$, $x_2 = -31/13$, $x_3 = -4/13$, $x_4 = 43/13$, $x_5 = 0$ son soluciones particulares del sistema.

Véanse también Problemas 16-18.

Estos ejemplos y problemas ilustran el

Teorema XVII. Un sistema de ecuaciones lineales no homogéneas sobre $\mathscr{F}$ en n incógnitas tiene una solución en $\mathscr{F}$ si, y solo si, la característica de su matriz coeficiente es igual a la característica de su matriz aumentada. Si la característica común es n, el sistema tiene una solución única. Si la característica común es $r < n$, se pueden dar valores arbitrarios

en $\mathscr{F}$ a $n - r$ de las incógnitas y entonces las restantes r incógnitas quedan univocamente determinadas en función de éstas.

Si $m = n$ en el sistema (7) podemos proceder como sigue:

(i) Escríbase el sistema en forma matricial $\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ x_n \end{bmatrix} = \begin{bmatrix} h_1 \\ h_2 \\ \cdot \\ h_n \end{bmatrix}$ o bien en forma más compacta, $A \cdot X = H$ donde X es la matriz $n \times 1$ de incógnitas y H es la matriz $n \times 1$ de términos constantes.

(ii) Procédase con la matriz A como al calcular A^{-1}. Si durante el proceso se obtiene una fila o columna de elementos nulos, A es singular y hay que comenzar de nuevo con la matriz $[A\ H]$ como en el primer procedimiento. Pero si A es regular con inversa A^{-1}, entonces $A^{-1}(A \cdot X) = A^{-1} \cdot H$ y $X = A^{-1} \cdot H$.

Ejemplo 20: Para el sistema del Ejemplo 18 tenemos, por el Ejemplo 14, $A^{-1} = \begin{bmatrix} -26 & -7 & 12 \\ 11 & 3 & -5 \\ -5 & -1 & 2 \end{bmatrix}$; entonces

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = A^{-1} \cdot H = \begin{bmatrix} -26 & -7 & 12 \\ 11 & 3 & -5 \\ -5 & -1 & 2 \end{bmatrix} \cdot \begin{bmatrix} -1 \\ 28 \\ 14 \end{bmatrix} = \begin{bmatrix} -2 \\ 3 \\ 5 \end{bmatrix}$$

y obtenemos la solución única como antes.

Sistemas de ecuaciones lineales homogéneas.

El sistema (7) se llama de *ecuaciones lineales homogéneas* si todo $h_i = 0$. Como entonces la característica de la matriz coeficiente es la misma que la de la matriz aumentada, el sistema tiene siempre una o más soluciones. Si la característica es n, entonces la *solución trivial* $x_1 = x_2 = \cdots = x_n = 0$ es la única solución; si la característica es $r < n$, el Teorema XVI' asegura la existencia de soluciones no triviales. Tenemos el

Teorema XVIII. Un sistema de ecuaciones lineales homogéneas sobre $\mathscr{F}$ en n incógnitas tiene siempre la solución trivial $x_1 = x_2 = \cdots = x_n = 0$. Si la característica de la matriz coeficiente es n, la solución trivial es la única solución; si la característica es $r < n$, se pueden dar valores arbitrarios en $\mathscr{F}$ a $n - r$ de las incógnitas y las restantes r incógnitas quedan univocamente determinadas en función de éstas.

Ejemplo 21: Resolver el sistema $\begin{cases} x_1 + 2x_2 - x_3 = 0 \\ 3x_1 + 8x_2 + 2x_3 = 0 \\ 4x_1 + 9x_2 - x_3 = 0 \end{cases}$ sobre Q.

Por el Ejemplo 18, $A \sim I_3$. Así, pues, $x_1 = x_2 = x_3 = 0$ es la única solución.

Ejemplo 22: Resolver el sistema $\begin{cases} x_1 + x_2 + x_3 + x_4 = 0 \\ 2x_1 + 3x_2 + 2x_3 + x_4 = 0 \\ 3x_1 + 4x_2 + 3x_3 + 2x_4 = 0 \end{cases}$ sobre Q.

Tenemos

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 3 & 2 & 1 \\ 3 & 4 & 3 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$ de característica 2

Haciendo $x_3 = s$, $x_4 = t$ con $s, t \in Q$, obtenemos las soluciones pedidas así: $x_1 = -s - 2t$, $x_2 = t$, $x_3 = s$, $x_4 = t$.

Véase también Problema 19.

DETERMINANTE DE UNA MATRIZ CUADRADA

A cada matriz cuadrada A sobre $\mathscr{F}$ se puede asociar un elemento único $a \in \mathscr{F}$. Este elemento a, llamado *determinante* de A, se denota bien por $\det A$ o bien por $|A|$. Considérese la matriz cuadrada de orden n

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}$$

y un producto

$$a_{1j_1} a_{2j_2} a_{3j_3} \dots a_{nj_n}$$

de n de sus elementos tomados de tal manera que de cada fila hay uno, y solo uno, y de cada columna uno, y solo uno. Nótese que los factores en este producto están ordenados de modo que los indices de fila (primeros subindices) aparecen en el orden natural, $1, 2, 3, \dots, n$. La sucesión de los indices de columna (segundos subindices) es una permutación

$$\rho = (j_1, j_2, j_3, \dots, j_n)$$

de los digitos $1, 2, 3, \dots, n$. Para esta permutación, defínase $\epsilon_\rho = +1$ o -1, según que ρ sea par o impar, y fórmese el producto provisto de signo

$$(a) \qquad \epsilon_\rho a_{1j_1} a_{2j_2} a_{3j_3} \dots a_{nj_n}$$

El conjunto S_n de todas las permutaciones de n simbolos contiene $n!$ elementos; de modo que se pueden formar $n!$ productos distintos del tipo (a). El determinante de A se define como la suma de estos $n!$ productos dotados de signo (llamados términos de $|A|$), es decir,

$$(b) \qquad |A| = \sum_{S_n} \epsilon_\rho a_{1j_1} a_{2j_2} a_{3j_3} \dots a_{nj_n}$$

Ejemplo 23:

(i) $$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \epsilon_{12} a_{11} a_{22} + \epsilon_{21} a_{12} a_{21} = a_{11} a_{22} - a_{12} a_{21}$$

Así, pues, el determinante de una matriz de orden 2 es el producto de los elementos diagonales de la matriz menos el producto de los elementos que no están en la diagonal.

(ii) $$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = \epsilon_{123} a_{11} a_{22} a_{33} + \epsilon_{132} a_{11} a_{23} a_{32} + \epsilon_{213} a_{12} a_{21} a_{33} + \epsilon_{231} a_{12} a_{23} a_{31} + \epsilon_{312} a_{13} a_{21} a_{32} + \epsilon_{321} a_{13} a_{22} a_{31}$$

$$= a_{11} a_{22} a_{33} - a_{11} a_{23} a_{32} - a_{12} a_{21} a_{33} + a_{12} a_{23} a_{31} + a_{13} a_{21} a_{32} - a_{13} a_{22} a_{31}$$

$$= a_{11}(a_{22} a_{33} - a_{23} a_{32}) - a_{12}(a_{21} a_{33} - a_{23} a_{31}) + a_{13}(a_{21} a_{32} - a_{22} a_{31})$$

$$= a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

$$= (-1)^{1+1} a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} + (-1)^{1+2} a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + (-1)^{1+3} a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

llamado desarrollo del determinante con respecto a su primera fila. Se deja al lector hacer el desarrollo con respecto a cada fila y cada columna.

PROPIEDADES DE LOS DETERMINANTES

En toda esta sección, A es la matriz cuadrada de orden n cuyo determinante $|A|$ viene dado por (b) de la sección precedente.

De (b) se sigue fácilmente

Teorema XIX. Si cada elemento de una fila (columna) de una matriz cuadrada A es cero, entonces $|A| = 0$.

Teorema XX. Si A es triangular superior (inferior) o diagonal, entonces $|A| = a_{11}a_{22}a_{33}\cdots a_{nn}$, producto de los elementos diagonales.

Teorema XXI. Si B se obtiene de A multiplicando su fila i (columna i) por un escalar no nulo k, es $|B| = k|A|$.

Veamos ahora (a) con más detalle. Como ρ es una aplicación de $S = \{1, 2, 3, \ldots, n\}$ en sí mismo, se puede expresar (véase Capitulo 1) como

$$\rho: \quad 1\rho = j_1,\ 2\rho = j_2,\ 3\rho = j_3,\ \ldots,\ n\rho = j_n$$

Con esta notación, (a) toma la forma

$$(a') \qquad \epsilon_\rho\, a_{1,1\rho}\, a_{2,2\rho}\, a_{3,3\rho} \ldots a_{n,n\rho}$$

y (b) toma la forma

$$(b') \qquad |A| = \sum_{S_n} \epsilon_\rho\, a_{1,1\rho}\, a_{2,2\rho}\, a_{3,3\rho} \ldots a_{n,n\rho}$$

Como S_n es un grupo, contiene la inversa

$$\rho^{-1}: \quad j_1\rho^{-1} = 1,\ j_2\rho^{-1} = 2,\ j_3\rho^{-1} = 3,\ \ldots,\ j_n\rho^{-1} = n$$

de ρ. Además, ρ y ρ^{-1} son ambas impares o ambas pares. Así, pues, (a) se puede escribir como

$$\epsilon_{\rho^{-1}}\, a_{j_1\rho^{-1},j_1}\, a_{j_2\rho^{-1},j_2}\, a_{j_3\rho^{-1},j_3} \ldots a_{j_n\rho^{-1},j_n}$$

y después de reordenar los factores para que los índices de columna queden en orden natural, como

$$(a'') \qquad \epsilon_{\rho^{-1}}\, a_{1\rho^{-1},1}\, a_{2\rho^{-1},2}\, a_{3\rho^{-1},3} \ldots a_{n\rho^{-1},n}$$

y (b) como

$$(b'') \qquad |A| = \sum_{S_n} \epsilon_{\rho^{-1}}\, a_{1\rho^{-1},1}\, a_{2\rho^{-1},2}\, a_{3\rho^{-1},3} \ldots a_{n\rho^{-1},n}$$

Para toda matriz cuadrada $A = [a_{ij}]$ se define la *transpuesta* de A, denotada por A^T como la matriz que se obtiene intercambiando las filas y columnas de A. Por ejemplo,

$$\text{si} \quad A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \quad \text{entonces} \quad A^T = \begin{bmatrix} a_{11} & a_{21} & a_{31} \\ a_{12} & a_{22} & a_{32} \\ a_{13} & a_{23} & a_{33} \end{bmatrix}$$

Escribamos, pues, $A^T = [a_{ij}^T]$ donde $a_{ij}^T = a_{ji}$ para todo i y j. Entonces el término de $|A^T|$

$$\begin{aligned} \epsilon_\rho\, a_{1,j_1}^T\, a_{2,j_2}^T\, a_{3,j_3}^T \ldots a_{n,j_n}^T &= \epsilon_\rho\, a_{j_1,1}\, a_{j_2,2}\, a_{j_3,3} \ldots a_{j_n,n} \\ &= \epsilon_\rho\, a_{1\rho,1}\, a_{2\rho,2}\, a_{3\rho,3} \ldots a_{n\rho,n} \end{aligned}$$

es por (b'') un término de $|A|$. Como esto es cierto para toda $\rho \in S_n$, queda demostrado el

Teorema XXII. Si A^T es la transpuesta de la matriz cuadrada A, entonces $|A^T| = |A|$.

Sea ahora A una matriz cuadrada y sea B la matriz obtenida multiplicando la fila i de A por un escalar no nulo k. Expresada por matrices elementales $B = H_i(k) \cdot A$; y, por el Teorema XXI,

$$|B| = |H_i(k) \cdot A| = k|A|$$

Pero $|H_i(k)| = k$; luego $|H_i(k) \cdot A| = |H_i(k)| \cdot |A|$. Por una demostración independiente o bien por el Teorema XXII, también tenemos

$$|A \cdot K_i(k)| = |A| \cdot |K_i(k)|$$

Denótese ahora por B la matriz que se obtiene de la A intercambiando sus columnas i y j y denótese por τ la transposición correspondiente (i, j). El efecto de τ sobre (a') es producir

$$(a''') \qquad \epsilon_{\rho\tau} a_{1,1\rho\tau} a_{2,2\rho\tau} a_{3,3\rho\tau} \cdots a_{n,n\rho\tau}$$

por tanto,

$$|B| = \sum_{S_n} \epsilon_{\rho\tau} a_{1,1\rho\tau} a_{2,2\rho\tau} a_{3,3\rho\tau} \cdots a_{n,n\rho\tau}$$

Pero $\sigma = \rho\tau \in S_n$ es par si ρ es impar e impar si ρ es par; de modo que $\epsilon_\sigma = -\epsilon_\rho$. Además, con τ fijo, hágase describir S_n a ρ; entonces σ describe S_n y así

$$|B| = \sum_{S_n} \epsilon_\sigma a_{1,1\sigma} a_{2,2\sigma} a_{3,3\sigma} \cdots a_{n,n\sigma} = -|A|$$

Queda demostrado el

Teorema XXIII. Si B se obtiene de A intercambiando dos cualesquiera de sus filas (columnas), entonces $|B| = -|A|$.

Como en el Teorema XXIII $B = A \cdot K_{ij}$ y $|K_{ij}| = -1$, tenemos $|A \cdot K_{ij}| = |A| \cdot |K_{ij}|$ y, por simetría, $|H_{ij} \cdot A| = |H_{ij}| \cdot |A|$.

De aquí se sigue de inmediato, excluyendo todo cuerpo de característica dos,

Teorema XXIV. Si dos filas (columnas) de A son idénticas, entonces $|A| = 0$.

Por último, sea B obtenida de A sumando a su fila i el producto por k (un escalar) de su fila j. Suponiendo $j < i$,

$$\begin{aligned} |B| &= \sum_{S_n} \epsilon_\rho a_{1,1\rho} \cdots a_{j,j\rho} \cdots a_{i-1,(i-1)\rho} (a_{i,i\rho} + k a_{j,j\rho}) a_{i+1,(i+1)\rho} \cdots a_{n,n\rho} \\ &= \sum_{S_n} \epsilon_\rho a_{1,1\rho} a_{2,2\rho} a_{3,3\rho} \cdots a_{n,n\rho} \\ &\qquad + \sum_{S_n} \epsilon_\rho a_{1,1\rho} \cdots a_{j,j\rho} \cdots a_{i-1,(i-1)\rho} (k a_{j,j\rho}) a_{i+1,(i+1)\rho} \cdots a_{n,n\rho} \\ &= |A| + 0 = |A| \qquad \text{(con } (b') \text{ y Teoremas XXI y XXIV)} \end{aligned}$$

Queda demostrado (el caso $j > i$ se deja al lector) el

Teorema XXV. Si B resulta de A por adición a su fila i del producto por k (un escalar) de su fila j, es $|B| = |A|$. Teorema que también es válido si se cambia «fila» por «columna».

Como en el Teorema XXV, $B = H_{ij}(k) \cdot A$ y $|H_{ij}(k)| = |I| = 1$, se tiene

$$|H_{ij}(k) \cdot A| = |H_{ij}(k)| \cdot |A| \quad \text{y} \quad |A \cdot K_{ij}(k)| = |A| \cdot |K_{ij}(k)|$$

Y ahora queda demostrado el

Teorema XXVI. Si A es una matriz cuadrada de orden n y $H(K)$ es una matriz elemental cuadrada por fila (columna) de orden n, entonces

$$|H \cdot A| = |H| \cdot |A| \quad \text{y} \quad |A \cdot K| = |A| \cdot |K|$$

Por el Teorema IX', toda matriz cuadrada A se puede expresar como

$$(c) \qquad A = H_1^{-1} \cdot H_2^{-1} \cdots H_s^{-1} \cdot N \cdot K_t^{-1} \cdots K_2^{-1} \cdot K_1^{-1}$$

Y entonces, por aplicaciones reiteradas del Teorema XXVI, se obtiene

$$\begin{aligned}|A| &= |H_1^{-1}| \cdot |H_2^{-1}| \cdots |H_s^{-1} \cdot N \cdot K_t^{-1} \cdots K_2^{-1} \cdot K_1^{-1}| \\ &= |H_1^{-1}| \cdot |H_2^{-1}| \cdot |H_3^{-1} \cdots H_s^{-1} \cdot N \cdot K_t^{-1} \cdots K_2^{-1} \cdot K_1^{-1}| \\ &= \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &= |H_1^{-1}| \cdot |H_2^{-1}| \cdots |H_s^{-1}| \cdot |N| \cdot |K_t^{-1}| \cdots |K_2^{-1}| \cdot |K_1^{-1}|\end{aligned}$$

Si A es regular, entonces $N = I$ y $|N| = 1$; si A es singular, entonces uno o más de los elementos diagonales de N es 0 y $|N| = 0$. Así, pues,

Teorema XXVII. Una matriz cuadrada A es regular si, y solo si, $|A| \neq 0$.

y

Teorema XXVIII. Si A y B son matrices cuadradas de orden n, entonces $|A \cdot B| = |A| \cdot |B|$.

CALCULO DE DETERMINANTES

Utilizando el resultado del Ejemplo 23 (ii), tenemos

$$\begin{aligned}\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 8 \end{vmatrix} &= (1)\begin{vmatrix} 5 & 6 \\ 7 & 8 \end{vmatrix} - (2)\begin{vmatrix} 4 & 6 \\ 5 & 8 \end{vmatrix} + (3)\begin{vmatrix} 4 & 5 \\ 5 & 7 \end{vmatrix} \\ &= (40 - 42) - 2(32 - 30) + 3(28 - 25) \\ &= -2 - 4 + 9 = 3\end{aligned}$$

El procedimiento más práctico para calcular $|A|$ de orden $n \geq 3$ consiste en reducir A a forma triangular mediante transformaciones elementales de los tipos $H_{ij}(k)$ y $K_{ij}(k)$ exclusivamente (no alteran el valor de $|A|$) y luego aplicando el Teorema XX. Si se usan otras transformaciones elementales, deben hacerse anotaciones cuidadosas, pues el efecto de H_{ij} o de K_{ij} es cambiar el signo de $|A|$ en tanto que el de $H_i(k)$ o de $K_j(k)$ es multiplicar $|A|$ por k.

Ejemplo 24: Observando las formas triangulares obtenidas en el Ejemplo 6 y en el Problema 8, se ve que mientras que los elementos diagonales no son únicos, el producto de los elementos diagonales lo es. En el Ejemplo 6(*a*), página 171, tenemos

$$|A| = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 8 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -3 & -7 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & 0 & -1 \end{vmatrix} = (1)(-3)(-1) = 3$$

Véase también Problema 20.

Problemas resueltos

1. Hallar la imagen de $\xi = (1, 2, 3, 4)$ por la transformación lineal $A = \begin{bmatrix} 1 & -2 & 0 & 4 \\ 2 & 4 & 1 & -2 \\ 0 & -1 & 5 & -1 \\ 1 & 3 & 2 & 0 \end{bmatrix}$ de $V_4(Q)$ en sí mismo.

$$\xi A = \xi[\gamma_1\ \gamma_2\ \gamma_3\ \gamma_4] = (\xi \cdot \gamma_1,\ \xi \cdot \gamma_2,\ \xi \cdot \gamma_3,\ \xi \cdot \gamma_4)$$

$$= (9, 15, 25, -3)$$ (Véase Problema 15, Capítulo 13, página 158.)

2. Calcular $A \cdot B$ y $B \cdot A$ dadas $A = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$ y $B = [4\ 5\ 6]$.

$$A \cdot B = \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \cdot [4\ 5\ 6] = \begin{bmatrix} 1\cdot4 & 1\cdot5 & 1\cdot6 \\ 2\cdot4 & 2\cdot5 & 2\cdot6 \\ 3\cdot4 & 3\cdot5 & 3\cdot6 \end{bmatrix} = \begin{bmatrix} 4 & 5 & 6 \\ 8 & 10 & 12 \\ 12 & 15 & 18 \end{bmatrix}$$

y $$B \cdot A = [4\ 5\ 6] \cdot \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = [4\cdot1 + 5\cdot2 + 6\cdot3] = [32] .$$

3. Si $A = \begin{bmatrix} 1 & 2 & -2 \\ 3 & 0 & 1 \end{bmatrix}$ y $B = \begin{bmatrix} 2 & 1 & 0 & -1 \\ 1 & 3 & -2 & 0 \\ 0 & 1 & -1 & -1 \end{bmatrix}$, Hallar $A \cdot B$.

$$A \cdot B = \begin{bmatrix} 2+2 & 1+6-2 & -4+2 & -1+2 \\ 6 & 3+1 & -1 & -3-1 \end{bmatrix} = \begin{bmatrix} 4 & 5 & -2 & 1 \\ 6 & 4 & -1 & -4 \end{bmatrix}$$

4. Demostrar que la transformación lineal $\begin{bmatrix} 1 & 2 & 2 & 0 \\ 2 & 5 & 3 & 1 \\ 3 & 8 & 4 & 2 \\ 2 & 7 & 1 & 3 \end{bmatrix}$ en $V_4(R)$ es singular y hallar un vector cuya imagen sea 0.

Utilizando sucesivamente $H_{21}(-2), H_{31}(-3), H_{41}(-2)$; $H_{12}(-2), H_{32}(-2), H_{42}(-3)$, se tiene

$$\begin{bmatrix} 1 & 2 & 2 & 0 \\ 2 & 5 & 3 & 1 \\ 3 & 8 & 4 & 2 \\ 2 & 7 & 1 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 2 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 2 & -2 & 2 \\ 0 & 3 & -3 & 3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 4 & -2 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

La transformación es singular, de característica 2.

Designense las matrices equivalentes por A, B, C, respectivamente, y denótense por $\rho_1, \rho_2, \rho_3, \rho_4$ los vectores fila de A, por $\rho_1', \rho_2', \rho_3', \rho_4'$ los vectores fila de B y por $\rho_1'', \rho_2'', \rho_3'', \rho_4''$ los vectores fila de C. Aplicando en orden los pasos, tenemos

$$\rho_2' = \rho_2 - 2\rho_1, \quad \rho_3' = \rho_3 - 3\rho_1, \quad \rho_4' = \rho_4 - 2\rho_1$$

$$\rho_1'' = \rho_1 - 2\rho_2', \quad \rho_3'' = \rho_3' - 2\rho_2', \quad \rho_4'' = \rho_4' - 3\rho_2'$$

Ahora bien, $\rho_3'' = \rho_3' - 2\rho_2' = (\rho_3 - 3\rho_1) - 2(\rho_2 - 2\rho_1) = \rho_3 - 2\rho_2 + \rho_1 = 0$

mientras que $\rho_4'' = \rho_4' - 3\rho_2' = (\rho_4 - 2\rho_1) - 3(\rho_2 - 2\rho_1) = \rho_4 - 3\rho_2 + 4\rho_1 = 0$

Así, pues, la imagen de $\xi = (1, -2, 1, 0)$ es 0; también la imagen de $\eta = (4, -3, 0, 1)$ es 0. Demostrar que los vectores cuya imagen es 0 llenan un subespacio de dimensión 2 en $V_4(R)$.

5. Demostrar que la transformación lineal $A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}$ es regular.

Encontramos

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 \\ 0 & -3 & -3 \\ 0 & -4 & -6 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \\ 0 & -4 & -8 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & -4 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = B$$

Los vectores fila de A son linealmente independientes; la transformación lineal A es regular.

6. Hallar la característica de la transformación lineal $A = \begin{bmatrix} 1 & 2 & 2 & 4 & 2 \\ 2 & 5 & 3 & 10 & 7 \\ 3 & 5 & 7 & 10 & 4 \end{bmatrix}$ de $V_3(R)$ en $V_5(R)$.

Hallamos

$$\begin{bmatrix} 1 & 2 & 2 & 4 & 2 \\ 2 & 5 & 3 & 10 & 7 \\ 3 & 5 & 7 & 10 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 2 & 4 & 2 \\ 0 & 1 & -1 & 2 & 3 \\ 0 & -1 & 1 & -2 & -2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 4 & 0 & -4 \\ 0 & 1 & -1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 4 & 0 & 0 \\ 0 & 1 & -1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} = B$$

Los vectores imagen son linealmente independientes; $r_A = 3$.

7. Del conjunto $\{(2, 5, 0, -3), (3, 2, 1, 2), (1, 2, 1, 0), (5, 6, 3, 2), (1, -2, -1, 2)\}$ de vectores de $V_4(R)$, elegir un subconjunto linealmente independiente máximo.

El conjunto dado es linealmente dependiente (¿por qué?). Hallamos

$$A = \begin{bmatrix} 2 & 5 & 0 & -3 \\ 3 & 2 & 1 & 2 \\ 1 & 2 & 1 & 0 \\ 5 & 6 & 3 & 2 \\ 1 & -2 & -1 & 2 \end{bmatrix} \sim \begin{bmatrix} 0 & 1 & -2 & -3 \\ 0 & -4 & -2 & 2 \\ 1 & 2 & 1 & 0 \\ 0 & -4 & -2 & 2 \\ 0 & -4 & -2 & 2 \end{bmatrix} \sim \begin{bmatrix} 0 & 1 & -2 & -3 \\ 0 & 0 & -10 & -10 \\ 1 & 0 & 5 & 6 \\ 0 & 0 & -10 & -10 \\ 0 & 0 & -10 & -10 \end{bmatrix}$$

$$\sim \begin{bmatrix} 0 & 1 & -2 & -3 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 5 & 6 \\ 0 & 0 & -10 & -10 \\ 0 & 0 & -10 & -10 \end{bmatrix} \sim \begin{bmatrix} 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = B$$

Examinando los pasos dados, es claro que los primeros tres vectores de A son combinaciones lineales de los tres vectores linealmente independientes de B (compruébese esto). Así, $\{(2, 5, 0, -3), (3, 2, 1, 2), (1, 2, 1, 0)\}$ es un subconjunto máximo linealmente independiente de A. ¿Se puede concluir que cualesquiera tres vectores de A son necesariamente linealmente independientes? Compruébese considerando el subconjunto $\{(1, 2, 1, 0), (5, 6, 3, 2), (1, -2, -1, 2)\}$.

8. Mediante transformaciones elementales de columna, reducir $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 8 \end{bmatrix}$ a triangular superior, triangular inferior y diagonal.

Con $K_{13}(-2/3), K_{23}(-5/6); K_{12}(1), K_{23}(-1/24)$, obtenemos

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 8 \end{bmatrix} \sim \begin{bmatrix} -1 & -1/2 & 3 \\ 0 & 0 & 6 \\ -1/3 & 1/3 & 3 \end{bmatrix} \sim \begin{bmatrix} -3/2 & -5/8 & 3 \\ 0 & -1/4 & 6 \\ 0 & 0 & 8 \end{bmatrix}$$ que es triangular superior.

Con $K_{21}(-2), K_{31}(-3); K_{32}(-2)$ obtenemos

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 5 & 7 & 8 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 4 & -3 & -6 \\ 5 & -3 & -7 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 4 & -3 & 0 \\ 5 & -3 & -1 \end{bmatrix}$$ que es triangular inferior.

Con $K_{21}(-2), K_{31}(-3), K_{32}(-2); K_{13}(5), K_{23}(-3); K_{12}(4/3)$ obtenemos

$$A \sim \begin{bmatrix} 1 & 0 & 0 \\ 4 & -3 & 0 \\ 5 & -3 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 4 & -3 & 0 \\ 0 & 0 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$ que es diagonal.

9. Demostrar: Toda matriz no nula A sobre $\mathscr{F}$ se puede reducir por sucesivas transformaciones elementales de fila a una matriz canónica por filas (matriz escalón) C con las propiedades siguientes:

(i) Cada una de las primeras r filas de C tiene por lo menos un elemento distinto de cero; las otras filas, si las hay, consisten enteramente en elementos cero.

(ii) En la fila i $(i = 1, 2, \ldots, r)$ de C, su primer elemento no nulo es 1, la unidad de $\mathscr{F}$. Numérese j_i la columna en que está este elemento.

(iii) El único elemento no nulo en la columna numerada j_i $(i = 1, 2, \ldots, r)$ es el elemento 1 en la fila i.

(iv) $j_1 < j_2 < \cdots < j_r$.

Considérese la primera columna no nula, numerada j_1, de A:

(*a*) Si $a_{1j_1} \neq 0$, empléese $H_1(a_{1j_1}^{-1})$ para reducirla a 1, si es preciso.

(*b*) Si $a_{1j_1} = 0$, pero $a_{pj_1} \neq 0$, empléese H_{1p} y procédase como en (*a*).

(*c*) Utilícense transformaciones del tipo $H_{ij}(k)$ para obtener ceros en todos los otros lugares de la columna j_1 si es preciso.

Si solamente en la primera fila de la matriz B que resulta aparecen elementos no nulos, entonces $B = C$; si no, hay un elemento no nulo en otro lugar de la columna numerada $j_2 > j_1$. Si $b_{2j_2} \neq 0$, utilícese $H_2(b_{2j_2}^{-1})$ como en (*a*) y procédase como en (*c*); si $b_{2j_2} = 0$, pero $b_{qj_2} \neq 0$, utilícese H_{2q} y procédase como en (*a*) y (*c*).

Si se presentan elementos no nulos solamente en las primeras dos filas de la matriz que resulta, hemos llegado a C; si no, hay una columna numerada $j_3 > j_2$ que tiene elementos no nulos en otro lugar de la columna. Si ... y así sucesivamente; al final debemos llegar a C.

10. Demostrar: La característica de fila y la característica de columna de una matriz A sobre $\mathscr{F}$ son iguales.

Considérese una matriz $m \times n$ y supóngase que tiene características r de fila y s de columna. Así que un subconjunto máximo de vectores columna linealmente independientes de esta matriz, consiste en s vectores. Intercambiando columnas, si es preciso, dispóngase de modo que las primeras s columnas sean linealmente independientes. Se deja al cuidado del lector demostrar que tales permutaciones de columnas no aumentan ni disminuyen la característica de fila de la matriz dada. Sin que se pierda generalidad, podemos suponer que en

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1s} & a_{1,s+1} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2s} & a_{2,s+1} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{s1} & a_{s2} & \cdots & a_{ss} & a_{s,s+1} & \cdots & a_{sn} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{ms} & a_{m,s+1} & \cdots & a_{mn} \end{bmatrix}$$

son linealmente independientes los primeros s vectores columna $\gamma_1, \gamma_2, \ldots, \gamma_s$ en tanto que cada uno de los restantes $n - s$ vectores columna es combinación lineal de éstos, por ejemplo,

$$\gamma_{s+t} = c_{1t}\gamma_1 + c_{2t}\gamma_2 + \cdots + c_{st}\gamma_s, \quad (t = 1, 2, \ldots, n-s)$$

con $c_{ij} \in \mathscr{F}$. Definanse los siguientes vectores:

$$\rho_1 = (a_{11}, a_{12}, \ldots, a_{1s}), \quad \rho_2 = (a_{21}, a_{22}, \ldots, a_{2s}), \quad \ldots, \quad \rho_m = (a_{m1}, a_{m2}, \ldots, a_{ms})$$

y $$\sigma_1 = (a_{11}, a_{21}, \ldots, a_{s+1,1}), \quad \sigma_2 = (a_{12}, a_{22}, \ldots, a_{s+1,2}), \quad \ldots, \quad \sigma_n = (a_{1n}, a_{2n}, \ldots, a_{s+1,n})$$

Como los ρ están en un espacio $V_s(\mathscr{F})$, cualesquiera $s + 1$ de ellos forman un conjunto linealmente dependiente. Así, pues, existen escalares $b_1, b_2, \ldots, b_{s+1}$ de $\mathscr{F}$ no todos nulos, tales que

$$\begin{aligned} b_1\rho_1 + b_2\rho_2 + \cdots + b_{s+1}\rho_{s+1} &= (b_1a_{11} + b_2a_{21} + \cdots + b_{s+1}a_{s+1,1}, \ b_1a_{12} + b_2a_{22} + \cdots \\ &\quad + b_{s+1}a_{s+1,2}, \ \ldots, \ b_1a_{1s} + b_2a_{2s} + \cdots + b_{s+1}a_{s+1,s}) \\ &= (\xi \cdot \sigma_1, \ \xi \cdot \sigma_2, \ \ldots, \ \xi \cdot \sigma_s) = \zeta \end{aligned}$$

donde $\zeta = (0, 0, \ldots, 0) = 0$ es el vector nulo de $V_s(\mathscr{F})$ y $\xi = (b_1, b_2, \ldots, b_{s+1})$. Entonces,

$$\xi \cdot \sigma_1 = \xi \cdot \sigma_2 = \cdots = \xi \cdot \sigma_s = 0$$

Considérese cualquiera de los restantes σ, por ejemplo,

$$\begin{aligned}\sigma_{s+k} &= (a_{1,s+k},\ a_{2,s+k},\ \ldots,\ a_{s+1,s+k}) \\ &= (c_{k1}a_{11} + c_{k2}a_{12} + \cdots + c_{ks}a_{1s},\ c_{k1}a_{21} + c_{k2}a_{22} + \cdots + c_{ks}a_{2s},\ \ldots, \\ &\qquad c_{k1}a_{s+1,1} + c_{k2}a_{s+1,2} + \cdots + c_{ks}a_{s+1,s})\end{aligned}$$

Entonces, $$\xi \cdot \sigma_{s+k} = c_{k1}(\xi \cdot \sigma_1) + c_{k2}(\xi \cdot \sigma_2) + \cdots + c_{ks}(\xi \cdot \sigma_s) = 0$$

Así que cualquier conjunto de $s + 1$ filas de A es linealmente dependiente; luego $s \leq r$, esto es,

la característica de columna de una matriz no puede exceder su característica de fila.

Para completar la demostración hemos de demostrar que $r \leq s$. Y esto puede hacerse de una de dos maneras:

(i) Repitiendo el razonamiento anterior comenzando con las filas linealmente independientes (las primeras r) en A, y deduciendo que sus primeras $r + 1$ columnas son linealmente dependientes.

(ii) Considérese la traspuesta de A

$$A^T = \begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \cdots & \cdots & \cdots & \cdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{bmatrix}$$

cuyas filas son las columnas correspondientes de A. Entonces, la característica de fila de A^T es s, la característica de columna de A, y la característica de columna de A^T es r, que es la característica de fila de A. Por el razonamiento anterior, la característica de columna de A^T no puede superar su característica de fila; es decir, $r \leq s$.

En cualquier caso, tenemos $r = s$, como se requería.

11. Reducir $A = \begin{bmatrix} 3 & 2 & 3 & 4 & 5 \\ 2 & -1 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & -3 \end{bmatrix}$ sobre R a forma normal.

Primero utilizamos $H_{12}(-1)$ para tener el elemento 1 en la primera fila y primera columna; así

$$A = \begin{bmatrix} 3 & 2 & 3 & 4 & 5 \\ 2 & -1 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & -3 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & -1 & -1 & 4 \\ 2 & -1 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & -3 \end{bmatrix}$$

Con $H_{21}(-2)$, $H_{31}(-4)$, $K_{21}(-3)$, $K_{31}(1)$, $K_{41}(1)$, $K_{51}(-4)$, tenemos

$$A \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & -7 & 6 & 7 & -7 \\ 0 & -7 & 5 & 6 & -19 \end{bmatrix}$$

Utilizando, entonces, $H_{32}(-1)$, $K_2(-1/7)$, $K_{32}(-6)$, $K_{42}(-7)$, $K_{52}(7)$, tenemos

$$A \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & -1 & -12 \end{bmatrix}$$

y, por último, con $H_3(-1)$, $K_{43}(-1)$, $K_{53}(-12)$,

$$A \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$A = \begin{bmatrix} 1 & 1 & 1 & 2 \\ 2 & 1 & -3 & -6 \\ 3 & 3 & 1 & 2 \end{bmatrix}$ sobre R a forma normal N y hallar matrices S y T tales que $S \cdot A \cdot T = N$.

Hallamos

$$I_4 \quad A \quad I_3 = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \\ \hline 1 & 1 & 1 & 2 & 1 & 0 & 0 \\ 2 & 1 & -3 & -6 & 0 & 1 & 0 \\ 3 & 3 & 1 & 2 & 0 & 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \\ \hline 1 & 1 & 1 & 2 & 1 & 0 & 0 \\ 0 & -1 & -5 & -10 & -2 & 1 & 0 \\ 0 & 0 & -2 & -4 & -3 & 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & -5 & -10 & -2 & 1 & 0 \\ 0 & 0 & -2 & -4 & -3 & 0 & 1 \end{array}\right]$$

$$\rightarrow \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 5 & 10 & 2 & -1 & 0 \\ 0 & 0 & 1 & 2 & 3/2 & 0 & -1/2 \end{array}\right] \rightarrow \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & & & \\ 0 & 1 & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -11/2 & -1 & 5/2 \\ 0 & 0 & 1 & 0 & 3/2 & 0 & -1/2 \end{array}\right] = N \quad S \qquad T$$

Luego $S = \begin{bmatrix} 1 & 0 & 0 \\ -11/2 & -1 & 5/2 \\ 3/2 & 0 & -1/2 \end{bmatrix}$ y $T = \begin{bmatrix} 1 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

13. Demostrar: El inverso del producto de dos matrices A y B, ambas dotadas de inversa, es el producto de las inversas en orden inverso, esto es,

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$$

Por definición, $(A \cdot B)^{-1} \cdot (A \cdot B) = (A \cdot B)(A \cdot B)^{-1} = I$. Ahora bien,

$$(B^{-1} \cdot A^{-1}) \cdot (A \cdot B) = B^{-1}(A^{-1} \cdot A)B = B^{-1} \cdot I \cdot B = B^{-1} \cdot B = I$$

y

$$(A \cdot B)(B^{-1} \cdot A^{-1}) = A(B \cdot B^{-1})A^{-1} = A \cdot A^{-1} = I$$

Como $(A \cdot B)^{-1}$ es único (véase Problema 33), tenemos $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.

14. Calcular la inversa de $A = \begin{bmatrix} 1 & 2 & 4 \\ 3 & 1 & 0 \\ 2 & 2 & 1 \end{bmatrix}$ sobre $Z/(5)$.

Tenemos

$$(A \quad I_3) = \left[\begin{array}{ccc|ccc} 1 & 2 & 4 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 1 & 0 \\ 2 & 2 & 1 & 0 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 2 & 4 & 1 & 0 & 0 \\ 0 & 0 & 3 & 2 & 1 & 0 \\ 0 & 3 & 3 & 3 & 0 & 1 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 2 & 4 & 1 & 0 & 0 \\ 0 & 3 & 3 & 3 & 0 & 1 \\ 0 & 0 & 3 & 2 & 1 & 0 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|ccc} 1 & 2 & 4 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 4 & 2 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 2 & 4 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 4 & 2 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 2 & 3 & 2 \\ 0 & 0 & 1 & 4 & 2 & 0 \end{array}\right]$$

y

$$A^{-1} = \begin{bmatrix} 1 & 1 & 1 \\ 2 & 3 & 2 \\ 4 & 2 & 0 \end{bmatrix}.$$

15. Hallar el polinomio mínimo de $A = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix}$ sobre R.

Es claro que $A \neq a_0 I$ para todo $a_0 \in R$. Póngase

$$A^2 = \begin{bmatrix} 2 & 4 & 2 \\ 0 & 4 & 0 \\ 2 & 4 & 2 \end{bmatrix} = a_1 \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix} + a_0 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} a_1 + a_0 & a_1 & a_1 \\ 0 & 2a_1 + a_0 & 0 \\ a_1 & a_1 & a_1 + a_0 \end{bmatrix}$$

que es imposible. Póngase ahora

$$A^3 = \begin{bmatrix} 4 & 12 & 4 \\ 0 & 8 & 0 \\ 4 & 12 & 4 \end{bmatrix} = a_2 \begin{bmatrix} 2 & 4 & 2 \\ 0 & 4 & 0 \\ 2 & 4 & 2 \end{bmatrix} + a_1 \begin{bmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix} + a_0 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 2a_2 + a_1 + a_0 & 4a_2 + a_1 & 2a_2 + a_1 \\ 0 & 4a_2 + 2a_1 + a_0 & 0 \\ 2a_2 + a_1 & 4a_2 + a_1 & 2a_2 + a_1 + a_0 \end{bmatrix}$$

De $\begin{cases} 2a_2 + a_1 + a_0 = 4 \\ 4a_2 + a_1 = 12, \\ 2a_2 + a_1 = 4 \end{cases}$ obtenemos $a_0 = 0$, $a_1 = -4$, $a_2 = 4$. Después de comprobar para todo elemento de A^3 y no antes, concluimos que $m(\lambda) = \lambda^3 - 4\lambda^2 + 4\lambda$.

16. Hallar todas las soluciones, si las hay, del sistema $\begin{cases} 2x_1 + 2x_2 + 3x_3 + x_4 = 1 \\ 3x_1 - x_2 + x_3 + 3x_4 = 2 \\ -2x_1 + 3x_2 - x_3 - 2x_4 = 4 \\ x_1 + 5x_2 + 3x_3 - 3x_4 = 2 \\ 2x_1 + 7x_2 + 3x_3 - 2x_4 = 8 \end{cases}$ sobre R.

Tenemos

$$[A\ H] = \begin{bmatrix} 2 & 2 & 3 & 1 & 1 \\ 3 & -1 & 1 & 3 & 2 \\ -2 & 3 & -1 & -2 & 4 \\ 1 & 5 & 3 & -3 & 2 \\ 2 & 7 & 3 & -2 & 8 \end{bmatrix} \sim \begin{bmatrix} 1 & 5 & 3 & -3 & 2 \\ 3 & -1 & 1 & 3 & 2 \\ -2 & 3 & -1 & -2 & 4 \\ 2 & 2 & 3 & 1 & 1 \\ 2 & 7 & 3 & -2 & 8 \end{bmatrix} \sim \begin{bmatrix} 1 & 5 & 3 & -3 & 2 \\ 0 & -16 & -8 & 12 & -4 \\ 0 & 13 & 5 & -8 & 8 \\ 0 & -8 & -3 & 7 & -3 \\ 0 & -3 & -3 & 4 & 4 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 5 & 3 & -3 & 2 \\ 0 & 1 & 1/2 & -3/4 & 1/4 \\ 0 & 13 & 5 & -8 & 8 \\ 0 & -8 & -3 & 7 & -3 \\ 0 & -3 & -3 & 4 & 4 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1/2 & 3/4 & 3/4 \\ 0 & 1 & 1/2 & -3/4 & 1/4 \\ 0 & 0 & -3/2 & 7/4 & 19/4 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & -3/2 & 7/4 & 19/4 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1/2 & 3/4 & 3/4 \\ 0 & 1 & 1/2 & -3/4 & 1/4 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & -3/2 & 7/4 & 19/4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 & 1/4 & 5/4 \\ 0 & 1 & 0 & -5/4 & 3/4 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 13/4 & 13/4 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 1/4 & 5/4 \\ 0 & 1 & 0 & -5/4 & 3/4 \\ 0 & 0 & 1 & 1 & -1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Tanto A como $[A\ H]$ tienen característica 4, el número de incógnitas. Hay una solución única: $x_1 = 1$, $x_2 = 2$, $x_3 = -2$, $x_4 = 1$.

Nota. El primer paso en la reducción fue H_{14}. Fue para tener el elemento 1 en la primera fila y primera columna, cosa que también se habría podido lograr con $H_1(\frac{1}{2})$.

17. Reducir $\begin{bmatrix} 3 & 2 & 1 \\ 6 & 5 & 4 \\ 4 & 2 & 5 \end{bmatrix}$ sobre $Z/(7)$ a forma normal.

Con $H_1(5)$; $H_{21}(1), H_{31}(3)$; $H_{12}(4), H_{32}(3)$; $H_3(3)$; $H_{13}(1), H_{23}(5)$, tenemos

$$\begin{bmatrix} 3 & 2 & 1 \\ 6 & 5 & 4 \\ 4 & 2 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & 5 \\ 6 & 5 & 4 \\ 4 & 2 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & 5 \\ 0 & 1 & 2 \\ 0 & 4 & 6 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 6 \\ 0 & 1 & 2 \\ 0 & 0 & 5 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 6 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

18. Hallar todas las soluciones, si las hay, del sistema $\begin{cases} x_1 + 2x_2 + x_3 + 3x_4 = 4 \\ 2x_1 + x_2 + 3x_3 + 2x_4 = 1 \\ 2x_2 + x_3 + x_4 = 3 \\ 3x_1 + x_2 + 3x_3 + 4x_4 = 2 \end{cases}$ sobre $Z/(5)$.

Tenemos

$$[A \;\; H] = \begin{bmatrix} 1 & 2 & 1 & 3 & 4 \\ 2 & 1 & 3 & 2 & 1 \\ 0 & 2 & 1 & 1 & 3 \\ 3 & 1 & 3 & 4 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 & 4 \\ 0 & 2 & 1 & 1 & 3 \\ 0 & 2 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 1 & 3 & 4 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 2 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 3 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Aquí, $r_A = r_{[A\,H]} = 2$; el sistema es compatible. Haciendo $x_3 = s$ y $x_4 = t$, con $s, t \in Z/(5)$, todas las soluciones vienen dadas por

$$x_1 = 1 + 3t, \quad x_2 = 4 + 2s + 2t, \quad x_3 = s, \quad x_4 = t$$

Como $Z/(5)$ es un cuerpo finito, solamente hay un número finito (hallarlo) de soluciones.

19. Resolver el sistema $\begin{cases} 2x_1 + x_2 + x_3 = 0 \\ x_1 + x_3 = 0 \\ 2x_2 + x_3 = 0 \end{cases}$ sobre $Z/(3)$.

Tenemos $$A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 2 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 2 \\ 1 & 0 & 1 \\ 0 & 2 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 2 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{bmatrix}$$

Entonces haciendo $x_3 = s \in Z/(3)$, obtenemos $x_1 = 2s$, $x_2 = x_3 = s$ como solución.

20. Con cada matriz sobre Q, calcular:

(a) $$\begin{vmatrix} 0 & 1 & -3 \\ 2 & 5 & 4 \\ -3 & 2 & -2 \end{vmatrix} = \begin{vmatrix} -1 & 1 & -3 \\ -3 & 5 & 4 \\ -5 & 2 & -2 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 0 \\ -3 & 2 & 13 \\ -5 & -3 & 13 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 0 \\ 2 & 5 & 0 \\ -5 & -3 & 13 \end{vmatrix} = -65$$

Se emplea $K_{12}(-1)$ para remplazar $a_{11} = 0$ por un elemento no nulo. El mismo resultado se puede obtener utilizando K_{12}; entonces,

$$\begin{vmatrix} 0 & 1 & -3 \\ 2 & 5 & 4 \\ -3 & 2 & -2 \end{vmatrix} = -\begin{vmatrix} 1 & 0 & -3 \\ 5 & 2 & 4 \\ 2 & -3 & -2 \end{vmatrix} = -\begin{vmatrix} 1 & 0 & 0 \\ 5 & 2 & 19 \\ 2 & -3 & 4 \end{vmatrix} = -\begin{vmatrix} 1 & 0 & 0 \\ 5 & 2 & 0 \\ 2 & -3 & 65/2 \end{vmatrix} = -65$$

Otra alternativa en el cálculo es la siguiente:

$$\begin{vmatrix} 0 & 1 & -3 \\ 2 & 5 & 4 \\ -3 & 2 & -2 \end{vmatrix} = \begin{vmatrix} 0 & 1 & 0 \\ 2 & 5 & 19 \\ -3 & 2 & 4 \end{vmatrix} = -(1)\begin{vmatrix} 2 & 19 \\ -3 & 4 \end{vmatrix} = -(8 + 57) = -65$$

$$(b)\quad \begin{vmatrix} 2 & 3 & -2 & 4 \\ 3 & -2 & 1 & 2 \\ 3 & 2 & 3 & 4 \\ -2 & 4 & 0 & 5 \end{vmatrix} = \begin{vmatrix} -1 & 3 & -2 & 4 \\ 5 & -2 & 1 & 2 \\ 1 & 2 & 3 & 4 \\ -6 & 4 & 0 & 5 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 0 & 0 \\ 5 & 13 & -9 & 22 \\ 1 & 5 & 1 & 8 \\ -6 & -14 & 12 & -19 \end{vmatrix}$$

$$= \begin{vmatrix} -1 & 0 & 0 & 0 \\ -1 & -1 & 3 & 3 \\ 1 & 5 & 1 & 8 \\ -6 & -14 & 12 & -19 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 1 & 5 & 16 & 23 \\ -6 & -14 & -30 & -61 \end{vmatrix} = \begin{vmatrix} -1 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 1 & 5 & 16 & 0 \\ -6 & -14 & -30 & -143/8 \end{vmatrix}$$

$$= (-1)(-1)(16)(-143/8) = -286$$

Problemas propuestos

21. Dadas $A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 3 & 1 \\ 4 & 2 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 1 & 4 & 3 \end{bmatrix}$, $C = \begin{bmatrix} -7 & 6 & -1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{bmatrix}$ sobre Q calcular:

(a) $A + B = \begin{bmatrix} 2 & 2 & 5 \\ 1 & 6 & 5 \\ 5 & 6 & 3 \end{bmatrix}$ (c) $A \cdot B = \begin{bmatrix} 3 & 10 & 9 \\ 4 & 13 & 15 \\ 6 & 14 & 20 \end{bmatrix}$ (e) $A \cdot C = \begin{bmatrix} -5 & 2 & 1 \\ 4 & -2 & -2 \\ -26 & 24 & -6 \end{bmatrix}$

(b) $3A = \begin{bmatrix} 3 & 0 & 6 \\ 0 & 9 & 3 \\ 12 & 6 & 0 \end{bmatrix}$ (d) $B \cdot C = \begin{bmatrix} -2 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{bmatrix}$ (f) $A^2 = A \cdot A = \begin{bmatrix} 9 & 4 & 2 \\ 4 & 11 & 3 \\ 4 & 6 & 10 \end{bmatrix}$

22. En el Problema 21 verificar: (a) $(A + B)C = AC + BC$, (b) $(A \cdot B)C = A(B \cdot C)$.

23. Para $A = [a_{ij}]$, $(i = 1, 2, 3;\ j = 1, 2, 3)$, calcular $I_3 \cdot A$ y $A \cdot I_3$ (igualmente $0_3 \cdot A$ y $A \cdot 0_3$) para comprobar que en el conjunto $\mathscr{R}$ de las matrices cuadradas de orden n sobre $\mathscr{F}$, la matriz nula y la matriz unidad conmutan con todos los elementos de $\mathscr{R}$.

24. Demostrar que el conjunto de todas las matrices de la forma $\begin{bmatrix} a & b & 0 \\ 0 & a+b & 0 \\ 0 & 0 & c \end{bmatrix}$ donde $a, b, c \in Q$ es una subálgebra de $\mathscr{M}_3(Q)$.

25. Demostrar que el conjunto de todas las matrices de la forma $\begin{bmatrix} a & b & c \\ 0 & a+c & 0 \\ c & b & a \end{bmatrix}$ donde $a, b, c \in R$, es una subálgebra de $\mathscr{M}_3(R)$.

26. Hallar la dimensión del espacio vectorial generado por cada uno de los conjuntos de vectores sobre Q siguientes. Elegir una base para cada uno.

(a) $\{(1, 4, 2, 4),\ (1, 3, 1, 2),\ (0, 1, 1, 2),\ (3, 8, 2, 4)\}$

(b) $\{(1, 2, 3, 4, 5),\ (5, 4, 3, 2, 1),\ (1, 0, 1, 0, 1),\ (3, 2, -1, -2, -5)\}$

(c) $\{(1, 1, 0, -1, 1),\ (1, 0, 1, 1, -1),\ (0, 1, 0, 1, 0),\ (1, 0, 0, 1, 1),\ (1, -1, 0, 1, 1)\}$

Resp. (a) 2, (b) 3, (c) 4

27. Demostrar que la transformación lineal $A = \begin{bmatrix} 1 & 2 & 3 & 0 \\ 2 & 4 & 3 & 1 \\ 3 & 2 & 1 & 4 \\ 2 & 0 & 4 & 2 \end{bmatrix}$ de $V_4(R)$ en sí mismo es singular y hallar un vector cuya imagen sea 0.

28. Demostrar: Las matrices cuadradas de orden 3 I, H_{12}, H_{13}, H_{23}, $H_{12} \cdot H_{13}$, $H_{12} \cdot H_{23}$ con la multiplicación forman un grupo isomorfo al grupo simétrico de 3 letras.

29. Demostrar: Con respecto a la multiplicación, el conjunto de las matrices cuadradas diagonales de orden n regulares sobre $\mathscr{F}$ es un grupo conmutativo.

30. Reducir las siguientes matrices sobre R a su matriz canónica equivalente por filas:

$$(a)\ \begin{bmatrix} 1 & 2 & -3 \\ 2 & 5 & -4 \end{bmatrix} \qquad (c)\ \begin{bmatrix} 1 & 2 & 1 & 2 \\ 1 & 3 & 2 & 2 \\ 2 & 4 & 3 & 4 \\ 3 & 7 & 4 & 6 \end{bmatrix} \qquad (e)\ \begin{bmatrix} 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 6 & 7 & 8 & 9 & 8 \\ 10 & 11 & 12 & 13 & 14 & 15 \end{bmatrix}$$

$$(b)\ \begin{bmatrix} 1 & 1 & 1 & 2 \\ 2 & 1 & -3 & -6 \\ 3 & 3 & 1 & 2 \end{bmatrix} \qquad (d)\ \begin{bmatrix} 1 & 2 & -2 & 3 \\ 2 & 5 & -4 & 6 \\ -1 & -3 & 2 & -2 \\ 2 & 4 & -1 & 6 \end{bmatrix}$$

Resp. $(a)\ \begin{bmatrix} 1 & 0 & -7 \\ 0 & 1 & 2 \end{bmatrix}$ $(b)\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{bmatrix}$ $(c)\ \begin{bmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ $(d)\ I_4$ $(e)\ \begin{bmatrix} 1 & 0 & -1 & -2 & -3 & 0 \\ 0 & 1 & 2 & 3 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$

31. En el Ejemplo 11, página 175, utilizar $H_2(\frac{1}{2})$, $H_{32}(-1)$, $H_{23}(-5)$, $K_3(2)$ sobre

$$\begin{array}{cccccc} 1 & -2 & 1 & & & \\ 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & & \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 5 & -3 & 1 & 0 \\ 0 & 1 & 3 & -4 & 0 & 1 \end{array}$$

y obténgase $S = \begin{bmatrix} 1 & 0 & 0 \\ 11 & 3 & -5 \\ -5/2 & -1/2 & 1 \end{bmatrix}$ y $T = \begin{bmatrix} 1 & -2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}$

para mostrar que las matrices regulares S y T tales que $S \cdot A \cdot T = I$ no son únicas.

32. Reducir $A = \begin{bmatrix} 1 & 2 & 3 & -2 \\ 2 & -2 & 1 & 3 \\ 3 & 0 & 4 & 1 \end{bmatrix}$ sobre R a forma normal N y determinar matrices S y T tales que $\cdot A \cdot T = N$.

33. Demostrar que si A es regular, su inversa A^{-1} es única.
Sugerencia: Suponer $A \cdot B = C \cdot A = I$ y considerar $(C \cdot A) \cdot B = C \cdot (A \cdot B)$.

34. Demostrar: Si A es regular, entonces $A \cdot B = A \cdot C$ implica $B = C$.

35. Demostrar que si las matrices regulares A y B conmutan, también lo hacen (a) A^{-1} y B, (b) A y B^{-1}, (c) A^{-1} y B^{-1}.
Sugerencia: (a) $A^{-1}(A \cdot B)A^{-1} = A^{-1}(B \cdot A)A^{-1}$.

36. Hallar la inversa de

$$(a)\ \begin{bmatrix} 1 & 3 & 3 \\ 1 & 4 & 3 \\ 1 & 3 & 4 \end{bmatrix} \qquad (c)\ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 3 \\ 2 & 4 & 3 \end{bmatrix} \qquad (e)\ \begin{bmatrix} 3 & 4 & 2 & 7 \\ 2 & 3 & 3 & 2 \\ 5 & 7 & 3 & 9 \\ 2 & 3 & 2 & 3 \end{bmatrix}$$

$$(b)\ \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 5 \\ 3 & 5 & 6 \end{bmatrix} \qquad (d)\ \begin{bmatrix} 2 & 1 & -1 \\ 1 & 3 & 2 \\ -1 & 2 & 1 \end{bmatrix} \qquad (f)\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & -4 \\ 2 & 3 & 5 & -5 \\ 3 & -4 & -5 & 8 \end{bmatrix}$$ sobre Q.

Resp. (*a*) $\begin{bmatrix} 7 & -3 & -3 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix}$, (*b*) $\begin{bmatrix} 1 & -3 & 2 \\ -3 & 3 & -1 \\ 2 & -1 & 0 \end{bmatrix}$, (*c*) $\frac{1}{3}\begin{bmatrix} 3 & -6 & 3 \\ -3 & 3 & 0 \\ 2 & 0 & -1 \end{bmatrix}$

(*d*) $\frac{1}{10}\begin{bmatrix} 1 & 3 & -5 \\ 3 & -1 & 5 \\ -5 & 5 & -5 \end{bmatrix}$, (*e*) $\frac{1}{2}\begin{bmatrix} -1 & 11 & 7 & -26 \\ -1 & -7 & -3 & 16 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & -1 & 2 \end{bmatrix}$, (*f*) $\frac{1}{18}\begin{bmatrix} 2 & 16 & -6 & 4 \\ 22 & 41 & -30 & -1 \\ -10 & -44 & 30 & -2 \\ 4 & -13 & 6 & -1 \end{bmatrix}$

37. Hallar la inversa de $A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 1 \end{bmatrix}$ sobre $Z/(3)$. ¿Tiene A inversa sobre $Z/(5)$?

Resp. $A^{-1} = \begin{bmatrix} 0 & 2 & 1 \\ 2 & 1 & 0 \\ 1 & 1 & 2 \end{bmatrix}$

38. Hallar el polinomio mínimo de (*a*) $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & -1 \end{bmatrix}$, (*b*) $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, (*c*) $\begin{bmatrix} 1 & 1 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 2 \end{bmatrix}$, (*d*) $\begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}$.

Resp. (*a*) $\lambda^3 + \lambda^2 - 2\lambda - 1$, (*b*) $\lambda^2 - 3\lambda + 2$, (*c*) $\lambda^2 - 4\lambda$, (*d*) $\lambda^2 - 5\lambda + 4$

39. Hallar la inversa de cada matriz (*a*), (*b*), (*d*) del Problema 36, mediante su polinomio mínimo.

40. Suponiendo que $\lambda^3 + a\lambda^2 + b\lambda$ es el polinomio mínimo de una matriz regular A, hacer ver una contradicción.

41. Demostrar los Teoremas XIX, XX y XXI, página 183.

42. Demostrar el Teorema XXIV. (*Sugerencia*: Si las filas i y j son idénticas en A, $|A| = |H_{ij}| \cdot |A|$.) Y también el Teorema XXVIII.

43. Calcular: $\det$.

(*a*) $\begin{vmatrix} 1 & 2 & 3 \\ 1 & 3 & 4 \\ 1 & 4 & 3 \end{vmatrix}$ (*c*) $\begin{vmatrix} -7 & 6 & -1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{vmatrix}$ (*e*) $\begin{vmatrix} 1 & 1 & 1 & 6 \\ 2 & 4 & 1 & 6 \\ 4 & 1 & 2 & 9 \\ 2 & 4 & 2 & 7 \end{vmatrix}$

(*b*) $\begin{vmatrix} 1 & 0 & 2 \\ 0 & 3 & 1 \\ 4 & 2 & 0 \end{vmatrix}$ (*d*) $\begin{vmatrix} 2 & -1 & 1 \\ 3 & 2 & 4 \\ -1 & 0 & 3 \end{vmatrix}$ (*f*) $\begin{vmatrix} 3 & 5 & 7 & 2 \\ 2 & 4 & 1 & 1 \\ -2 & 0 & 0 & 0 \\ 1 & 1 & 3 & 4 \end{vmatrix}$

Resp. (*a*) -2, (*b*) -26, (*c*) 4, (*d*) 27, (*e*) 41, (*f*) 156

44. Calcular: (*a*) $\begin{vmatrix} \lambda-1 & 2 & 3 \\ 1 & \lambda-3 & 4 \\ 1 & 4 & \lambda-3 \end{vmatrix}$, (*b*) $\begin{vmatrix} \lambda-2 & -1 & -4 \\ -1 & \lambda-3 & -5 \\ -4 & -5 & \lambda-6 \end{vmatrix}$

Sugerencia: Desarrollar por la primera fila o por la primera columna.

Resp. (*a*) $\lambda^3 - 7\lambda^2 - 6\lambda + 42$, (*b*) $\lambda^3 - 11\lambda^2 - 6\lambda + 28$

45. Denótense los vectores fila de $A = [a_{ij}]$, $(i, j = 1, 2, 3)$ por ρ_1, ρ_2, ρ_3. Demostrar que

(*a*) $\rho_1 \times \rho_2$ (véase Problema 13, Capítulo 13, página 157) se puede hallar como sigue: Escríbase el cuadro

$$\begin{matrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \end{matrix}$$

y táchese la primera columna. Entonces,

$$\rho_1 \times \rho_2 = \left(\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}, \begin{vmatrix} a_{13} & a_{11} \\ a_{23} & a_{21} \end{vmatrix}, \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \right)$$

(*b*) $|A| = \rho_1 \cdot (\rho_2 \times \rho_3) = -\rho_2 \cdot (\rho_1 \times \rho_3) = \rho_3 \cdot (\rho_1 \times \rho_2)$.

46. Demostrar que el conjunto de formas lineales

$$(a) \qquad \begin{cases} f_1 = a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ f_2 = a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_m = a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{cases} \quad \text{sobre } \mathcal{F}$$

es linealmente dependiente si, y solo si, la matriz coeficiente

$$A = [a_{ij}], \quad (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n)$$

es de característica $r < m$. Así, pues, (a) es necesariamente linealmente dependiente si $m > n$.

47. Hallar todas las soluciones de

$$(a)\ x_1 - 2x_2 + 3x_3 - 5x_4 = 1 \qquad (b)\ \begin{cases} x_1 + x_2 + x_3 = 4 \\ 2x_1 + 5x_2 - 2x_3 = 3 \end{cases} \qquad (c)\ \begin{cases} x_1 + x_2 + x_3 = 4 \\ 2x_1 + 5x_2 - 2x_3 = 3 \\ x_1 + 7x_2 - 7x_3 = 5 \end{cases}$$

$$(d)\ \begin{cases} 2x_1 + x_2 + 5x_3 + x_4 = 5 \\ x_1 + x_2 - 3x_3 - 4x_4 = -1 \\ 3x_1 + 6x_2 - 2x_3 + x_4 = 8 \\ 2x_1 + 2x_2 + 2x_3 - 3x_4 = 2 \end{cases} \qquad (e)\ \begin{cases} x_1 + x_2 + 2x_3 + x_4 = 5 \\ 2x_1 + 3x_2 - x_3 - 2x_4 = 2 \\ 4x_1 + 5x_2 + 3x_3 = 7 \end{cases}$$

$$(f)\ \begin{cases} x_1 + x_2 - 2x_3 + x_4 + 3x_5 = 1 \\ 2x_1 - x_2 + 2x_3 + 2x_4 + 6x_5 = 2 \\ 3x_1 + 2x_2 - 4x_3 - 3x_4 - 9x_5 = 3 \end{cases} \qquad (g)\ \begin{cases} x_1 + 3x_2 + x_3 + x_4 + 2x_5 = 0 \\ 2x_1 + 5x_2 - 3x_3 + 2x_4 - x_5 = 3 \\ -x_1 + x_2 + 2x_3 - x_4 + x_5 = 5 \\ 3x_1 + x_2 + x_3 - 2x_4 + 3x_5 = 0 \end{cases} \quad \text{sobre } Q.$$

Resp. $(a)\ x_1 = 1 + 2r - 3s + 5t,\ x_2 = r,\ x_3 = s,\ x_4 = t$

$(b)\ x_1 = 17/3 - 7r/3,\ x_2 = -5/3 + 4r/3,\ x_3 = r$

$(d)\ x_1 = 2,\ x_2 = 1/5,\ x_3 = 0,\ x_4 = 4/5$

$(f)\ x_1 = 1,\ x_2 = 2r,\ x_3 = r,\ x_4 = -3b,\ x_5 = b$

$(g)\ x_1 = -11/5 - 4r/5,\ x_2 = 2,\ x_3 = -1 - r,\ x_4 = -14/5 - r/5,\ x_5 = r$

48. (a) Demostrar que el conjunto $M_2 = \{A, B, \ldots\}$ de las matrices sobre Q de orden 2 es isomorfo al espacio vectorial $V_4(Q)$. *Sugerencia*: Usar $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \to (a_{11}, a_{12}, a_{21}, a_{22})$. Véase Problema 3, Capítulo 10, página 108.

(b) Demostrar que $I_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$, $I_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$, $I_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$, $I_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ es una base del espacio vectorial.

(c) Demostrar: A conmuta con $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$ si, y solo si, A conmuta con toda I_{ij} de (b).

Sugerencia: $B = b_{11}I_{11} + b_{12}I_{12} + b_{21}I_{21} + b_{22}I_{22}$.

49. Definase $S_2 = \left\{ \begin{bmatrix} x & y \\ -y & x \end{bmatrix} : x, y \in R \right\}$. Demuéstrese que (a) S_2 es un espacio vectorial sobre R, (b) S_2 es un cuerpo.

Sugerencia: En (b) muéstrese que la aplicación $S_2 \to C : \begin{bmatrix} x & y \\ -y & x \end{bmatrix} \to x + yi$ es un isomorfismo.

50. Demuéstrese que el conjunto $\mathcal{Q} = \{(q_1 + q_2 i + q_3 j + q_4 k) : q_1, q_2, q_3, q_4 \in R\}$ con la adición y multiplicación definidas en el Problema 27, Capítulo 11, página 123, es isomorfo al conjunto

$$S_4 = \left\{ \begin{bmatrix} q_1 & q_2 & q_3 & q_4 \\ -q_2 & q_1 & -q_4 & q_3 \\ -q_3 & q_4 & q_1 & -q_2 \\ -q_4 & -q_3 & q_2 & q_1 \end{bmatrix} : q_1, q_2, q_3, q_4 \in R \right\}$$

¿Es S_4 un cuerpo?

51. Demostrar: Si $\xi_1, \xi_2, \ldots, \xi_m$ son $m < n$ vectores linealmente independientes de $V_n(\mathscr{F})$, los p vectores

$$\eta_j = s_{j1}\xi_1 + s_{j2}\xi_2 + \cdots + s_{jm}\xi_m, \qquad (j = 1, 2, \ldots, p)$$

son linealmente dependientes si $p > m$ o bien, cuando $p \leq m$, si $[s_{ij}]$ es de característica $r < p$.

52. Demostrar: Si $\xi_1, \xi_2, \ldots, \xi_n$ son vectores linealmente independientes de $V_n(\mathscr{F})$, los n vectores

$$\eta_j = a_{j1}\xi_1 + a_{j2}\xi_2 + \cdots + a_{jn}\xi_n, \qquad (j = 1, 2, \ldots, n)$$

son linealmente independientes si, y solo si, $[a_{ij}] \neq 0$.

53. Verificar que el anillo $T_2 = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in R \right\}$ tiene los subanillos

$$\left\{ \begin{bmatrix} 0 & x \\ 0 & 0 \end{bmatrix} : x \in R \right\}, \quad \left\{ \begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} : x, y \in R \right\}, \quad \text{y} \quad \left\{ \begin{bmatrix} 0 & x \\ 0 & y \end{bmatrix} : x, y \in R \right\}$$

como sus ideales propios. Escribir el homomorfismo que determina a cada uno como un ideal. (Véase Teorema VI, Capítulo 10, página 105.)

54. Demostrar: $(A + B)^T = A^T + B^T$ y $(A \cdot B)^T = B^T \cdot A^T$ si A y B son matrices cuadradas de orden n sobre $\mathscr{F}$.

55. Considérense los vectores X y Y de n componentes como matrices $1 \times n$ y compruébese que

$$X \cdot Y = X \cdot Y^T = Y \cdot X^T$$

56. (*a*) Demostrar que el conjunto de matrices cuadradas de orden 4

$$\mathscr{M} = \{I, H_{12}, H_{13}, H_{14}, H_{23}, H_{24}, H_{34}, H_{12} \cdot H_{13}, H_{12} \cdot H_{23}, H_{12} \cdot H_{14}, H_{12} \cdot H_{24}, H_{13} \cdot H_{14}, H_{14} \cdot H_{13}, H_{23} \cdot H_{24}, H_{24} \cdot H_{23}, H_{12} \cdot H_{34}, H_{13} \cdot H_{24}, H_{14} \cdot H_{23}, H_{12} \cdot H_{13} \cdot H_{14}, H_{12} \cdot H_{14} \cdot H_{13}, H_{13} \cdot H_{12} \cdot H_{14}, H_{13} \cdot H_{14} \cdot H_{12}, H_{14} \cdot H_{12} \cdot H_{13}, H_{14} \cdot H_{13} \cdot H_{12}\}$$

es un grupo multiplicativo. *Sugerencia*: Mostrar que la aplicación

$$H_{ij} \to (ij), \quad H_{ij} \cdot H_{ik} \to (ijk), \quad H_{ij} \cdot H_{kl} \to (ij)(kl), \quad H_{ij} \cdot H_{ik} \cdot H_{il} \to (ijkl)$$

de $\mathscr{M}$ en S_n es un isomorfismo.

(*b*) Demostrar que el subconjunto $\{I, H_{13}, H_{24}, H_{12} \cdot H_{34}, H_{13} \cdot H_{24}, H_{14} \cdot H_{23}, H_{12} \cdot H_{13} \cdot H_{14}, H_{14} \cdot H_{13} \cdot H_{12}\}$ de $\mathscr{M}$ es un grupo isomorfo al grupo octal de un cuadrado. (En la Fig. 9-1, página 92, designar los vértices 1, 2, 3, 4 por (1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0) y (0, 0, 0, 1) respectivamente.)

57. Demostrar que el conjunto de matrices cuadradas de orden 2

$$\left\{ I, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}$$

es un grupo multiplicativo isomorfo al grupo octal de un cuadrado.
Sugerencia: Sitúese el cuadrado de la Fig. 9-1, página 92, en un sistema de coordenadas rectangular de modo que los vértices 1, 2, 3, 4 tengan coordenadas $(1, -1)$, $(1, 1)$, $(-1, 1)$, $(-1, -1)$ respectivamente.

58. Sean S generado por $(1, 0, 1, -1)$, $(1, 0, 2, 3)$, $(3, 0, 2, -1)$, $(1, 0, -2, -7)$ y T generado por $(2, 1, 3, 2)$, $(0, 4, -1, 0)$, $(2, 3, -4, 2)$, $(2, 4, -1, 2)$ subespacios de $V_4(Q)$. Hallar bases para S, T, $S \cap T$ y $S + T$.

Capítulo 15

Polinomios de matrices

MATRICES CON ELEMENTOS POLINOMIOS

Sea $\mathscr{F}[\lambda]$ el dominio de polinomios que consiste en todos los polinomios en λ con coeficientes en $\mathscr{F}$. Una matriz $m \times n$ sobre $\mathscr{F}[\lambda]$, es decir, cuyos elementos son polinomios de $\mathscr{F}[\lambda]$,

$$A(\lambda) = [a_{ij}(\lambda)] = \begin{bmatrix} a_{11}(\lambda) & a_{12}(\lambda) & \dots & a_{1n}(\lambda) \\ a_{21}(\lambda) & a_{22}(\lambda) & \dots & a_{2n}(\lambda) \\ \dots & \dots & \dots & \dots \\ a_{m1}(\lambda) & a_{m2}(\lambda) & \dots & a_{mn}(\lambda) \end{bmatrix}$$

se dice una matriz λ (léase matriz lambda).

Como $\mathscr{F} \subset \mathscr{F}[\lambda]$, el conjunto de todas las matrices $m \times n$ sobre $\mathscr{F}$ es un subconjunto del conjunto de todas las matrices λ sobre $\mathscr{F}[\lambda]$. Es, pues, de esperar que gran parte de lo dicho en el Capítulo 14 se verifique aquí, con cambios ligeros a lo más. Por ejemplo, con adición y multiplicación definidas sobre el conjunto de las matrices λ cuadradas de orden n sobre $\mathscr{F}[\lambda]$, se encuentra sin dificultad que este conjunto es también un anillo no conmutativo con unidad I_n, precisamente como ocurre con el conjunto de todas las matrices cuadradas de orden n sobre $\mathscr{F}$. Por otra parte, si bien $A(\lambda) = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda+1 \end{bmatrix}$ es regular, es decir, $|A(\lambda)| = \lambda(\lambda + 1) \neq 0$, $A(\lambda)$ no tiene inversa sobre $\mathscr{F}[\lambda]$. La razón es, desde luego, que en general $\alpha(\lambda)$ no tiene simétrica multiplicativa en $\mathscr{F}[\lambda]$. Así que resulta imposible generalizar la noción de transformaciones elementales a las matrices λ de modo que, por ejemplo

$$A(\lambda) = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda+1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

TRANSFORMACIONES ELEMENTALES

Se definen como sigue las transformaciones elementales de matrices λ:

El intercambio de las filas i y j, denotado por H_{ij}; el intercambio de las columnas i y j, denotado por K_{ij}.

La multiplicación de la fila i por un elemento $k \in \mathscr{F}$ diferente de cero, denotada por $H_i(k)$; la multiplicación de la columna i por un elemento $k \in \mathscr{F}$ diferente de cero, denotada por $K_i(k)$.

La adición a la fila i del producto de $f(\lambda) \in \mathscr{F}[\lambda]$ por la fila j, denotada por $H_{ij}(f(\lambda))$; la adición a la columna i del producto de $f(\lambda) \in \mathscr{F}[\lambda]$ por la columna j, denotada por $K_{ij}(f(\lambda))$.

(Obsérvese que las dos primeras transformaciones son idénticas a las del Capítulo 14, en tanto que la tercera permite multiplicar por todo elemento de $\mathscr{F}[\lambda]$.)

Se denotarán por el mismo símbolo una transformación elemental y la matriz elemental obtenida aplicando esa transformación a I. Así una transformación de fila de $A(\lambda)$ se efectúa multiplicándola a la izquierda por la H adecuada, y una transformación de columna se efectúa multiplicándola a la derecha por la K adecuada.

En correspondencia con los resultados del Capítulo 14 enunciamos:

Toda matriz elemental es regular.

El determinante de toda matriz elemental es un elemento de $\mathscr{F}$.

Toda matriz elemental tiene una inversa que, a su vez, es una matriz elemental.

Dos matrices λ $m \times n$ $A(\lambda)$ y $B(\lambda)$ se dicen equivalentes si la una puede obtenerse de la otra mediante sucesivas transformaciones elementales de fila y columna, es decir, si existen matrices $S(\lambda) = H_s \ldots H_2 \cdot H_1$ y $T(\lambda) = K_1 \cdot K_2 \ldots K_t$ tales que

$$S(\lambda) \cdot A(\lambda) \cdot T(\lambda) = B(\lambda)$$

La característica de fila (columna) de una matriz λ es el número de filas (columnas) linealmente independientes de la matriz. La característica de una matriz λ es su característica de fila (columna).

Matrices λ equivalentes tienen igual característica; la recíproca no es cierta.

FORMA NORMAL DE UNA MATRIZ – λ

En correspondencia con el Teorema IX', Capítulo 14, página 174, se tiene el

Teorema I. Toda matriz λ $A(\lambda)$ $m \times n$ sobre $\mathscr{F}[\lambda]$ de característica r se puede reducir por transformaciones elementales a una forma canónica (*forma normal*)

$$N(\lambda) = \begin{bmatrix} f_1(\lambda) & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ 0 & f_2(\lambda) & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & f_r(\lambda) & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

en la que $f_1(\lambda), f_2(\lambda), \ldots, f_r(\lambda)$ son polinomios mónicos de $\mathscr{F}[\lambda]$ y $f_i(\lambda)$ divide a $f_{i+1}(\lambda)$ para $i = 1, 2, \ldots, r-1$.

No vamos a demostrar este teorema ni que la forma normal de una $A(\lambda)$ dada es única. (La demostración del teorema consiste en mostrar cómo se llega a $N(\lambda)$ para una $A(\lambda)$ dada; la unicidad exige mayor estudio de los determinantes.) Un procedimiento sencillo para obtener la forma normal se ilustra en el ejemplo y problemas que siguen.

Ejemplo 1:

$$\text{Reducir } A(\lambda) = \begin{bmatrix} \lambda+3 & \lambda+1 & \lambda+2 \\ 2\lambda^2+\lambda-3 & \lambda^2+\lambda-1 & 2\lambda^2-2 \\ \lambda^3+\lambda^2+6\lambda+3 & 2\lambda^2+2\lambda+1 & \lambda^3+\lambda^2+5\lambda+2 \end{bmatrix}$$

sobre $R(\lambda)$ a forma normal.

El máximo común divisor de los elementos de $A(\lambda)$ es 1; tómese $f_1(\lambda) = 1$. Valiéndose ahora de $K_{13}(-1)$ remplácese $a_{11}(\lambda)$ por $f_1(\lambda)$ y luego, mediante transformaciones adecuadas de fila y columna, obténgase una matriz equivalente cuyas primeras fila y columna tienen nulos todos los elementos excepto el elemento común $f_1(\lambda)$; así se llega a

$$A(\lambda) \sim \begin{bmatrix} 1 & \lambda+1 & \lambda+2 \\ \lambda-1 & \lambda^2+\lambda-1 & 2\lambda^2-2 \\ \lambda+1 & 2\lambda^2+2\lambda+1 & \lambda^3+\lambda^2+5\lambda+2 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ \lambda-1 & \lambda & \lambda^2-\lambda \\ \lambda+1 & \lambda^2 & \lambda^3+2\lambda \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & \lambda^2-\lambda \\ 0 & \lambda^2 & \lambda^3+2\lambda \end{bmatrix} = B(\lambda)$$

Considérese ahora la submatriz $\begin{bmatrix} \lambda & \lambda^2-\lambda \\ \lambda^2 & \lambda^3+2\lambda \end{bmatrix}$. El máximo común divisor de sus elementos es λ; hágase $f_2(\lambda) = \lambda$. Como $f_2(\lambda)$ ocupa la posición de $b_{22}(\lambda)$ en $B(\lambda)$ procedemos a eliminar de la segunda fila y de la segunda columna los elementos no nulos, exceptuando, naturalmente, el elemento común $f_2(\lambda)$, y tenemos

$$A(\lambda) \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & \lambda^2-\lambda \\ 0 & \lambda^2 & \lambda^3+2\lambda \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & \lambda^2-\lambda \\ 0 & 0 & \lambda^2+2\lambda \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^2+2\lambda \end{bmatrix} = N(\lambda)$$

ya que $\lambda^2 + 2\lambda$ es mónico. Véanse también Problemas 1-3.

Los elementos no nulos de $N(\lambda)$, la forma normal de $A(\lambda)$ se llaman *factores invariantes* de $A(\lambda)$. Suponiendo que la forma normal de una matriz λ es única, se tiene el

Teorema II. Dos matrices λ $m \times n$ sobre $\mathscr{F}[\lambda]$ son equivalentes si, y solo si, tienen los mismos factores invariantes.

POLINOMIOS CON COEFICIENTES MATRICIALES

En lo que queda de este capítulo nos limitaremos a matrices λ cuadradas de orden n sobre $\mathscr{F}[\lambda]$. Sea $A(\lambda)$ una matriz semejante y supóngase que el grado máximo de todos los elementos polinomios $a_{ij}(\lambda)$ de $A(\lambda)$ es p. Por adición, cuando fuere necesario, de términos con coeficientes cero, $A(\lambda)$ puede escribirse de modo que cada uno de sus elementos tenga $p + 1$ términos. Entonces, $A(\lambda)$ se escribe como un polinomio de grado p en λ con matrices cuadradas A_i sobre $\mathscr{F}$ como coeficientes y se llama entonces *polinomio de matrices de grado p* en λ.

Ejemplo 2:

Para la matriz λ $A(\lambda)$ del Ejemplo 1, tenemos

$$A(\lambda) = \begin{bmatrix} \lambda+3 & \lambda+1 & \lambda+2 \\ 2\lambda^2+\lambda-3 & \lambda^2+\lambda-1 & 2\lambda^2-2 \\ \lambda^3+\lambda^2+6\lambda+3 & 2\lambda^2+2\lambda+1 & \lambda^3+\lambda^2+5\lambda+2 \end{bmatrix}$$

$$= \begin{bmatrix} 0\lambda^3+0\lambda^2+\lambda+3 & 0\lambda^3+0\lambda^2+\lambda+1 & 0\lambda^3+0\lambda^2+\lambda+2 \\ 0\lambda^3+2\lambda^2+\lambda-3 & 0\lambda^3+\lambda^2+\lambda-1 & 0\lambda^3+2\lambda^2+0\lambda-2 \\ \lambda^3+\lambda^2+6\lambda+3 & 0\lambda^3+2\lambda^2+2\lambda+1 & \lambda^3+\lambda^2+5\lambda+2 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}\lambda^3 + \begin{bmatrix} 0 & 0 & 0 \\ 2 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}\lambda^2 + \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 6 & 2 & 5 \end{bmatrix}\lambda + \begin{bmatrix} 3 & 1 & 2 \\ -3 & -1 & -2 \\ 3 & 1 & 2 \end{bmatrix}$$

Considérense ahora las matrices λ cuadradas de orden n o polinomios de matrices

$$A(\lambda) = A_p\lambda^p + A_{p-1}\lambda^{p-1} + \cdots + A_1\lambda + A_0 \qquad (1)$$

y

$$B(\lambda) = B_q\lambda^q + B_{q-1}\lambda^{q-1} + \cdots + B_1\lambda + B_0 \qquad (2)$$

Las dos matrices λ (polinomios de matrices) se dicen *iguales* si $p = q$ y $A_i = B_i$ para $i = 0, 1, 2, \ldots, p$.

La suma $A(\lambda) + B(\lambda)$ es una matriz λ (polinomio de matrices) que resulta de la adición de los elementos correspondientes (términos) de las matrices λ (polinomios de matrices). Si $p > q$, su grado es p: si $p = q$, su grado es a lo más p.

El producto $A(\lambda) \cdot B(\lambda)$ es una matriz λ (polinomio de matrices) de grado $p + q$ a lo más. Si $A(\lambda)$ o $B(\lambda)$ es regular (esto es, si $|A(\lambda)| \neq 0$ o $|B(\lambda)| \neq 0$), entonces $A(\lambda) \cdot B(\lambda)$ y $B(\lambda) \cdot A(\lambda)$ son de grado $p + q$. Como, en general, las matrices no conmutan, es de esperar que $A(\lambda) \cdot B(\lambda) \neq B(\lambda) \cdot A(\lambda)$.

La igualdad en (1) no se altera si λ se sustituye por cualquier $k \in \mathscr{F}$. Por ejemplo,

$$A(k) = A_p k^p + A_{p-1} k^{p-1} + \cdots + A_1 k + A_0$$

Pero si λ se sustituye por una matriz cuadrada C sobre $\mathscr{F}$, de orden n, se obtienen dos resultados que son, por lo general, distintos

$$A_R(C) = A_p C^p + A_{p-1} C^{p-1} + \cdots + A_1 C + A_0 \qquad (3)$$

y

$$A_L(C) = C^p A_p + C^{p-1} A_{p-1} + \cdots + C A_1 + A_0 \qquad (3')$$

llamados respectivamente valores funcionales a *derecha* y a *izquierda* de $A(\lambda)$ cuando $\lambda = C$.

Ejemplo 3:

$$\text{Si} \quad A(\lambda) = \begin{bmatrix} \lambda^2 & \lambda - 1 \\ \lambda + 3 & \lambda^2 + 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \lambda^2 + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \lambda + \begin{bmatrix} 0 & -1 \\ 3 & 2 \end{bmatrix} \quad \text{y} \quad C = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix},$$

$$\text{entonces} \quad A_R(C) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}^2 + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} + \begin{bmatrix} 0 & -1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 7 & 10 \\ 12 & 17 \end{bmatrix}$$

$$\text{y} \quad A_L(C) = \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix}^2 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & -1 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 14 & 17 \end{bmatrix}$$

Véase también Problema 4.

ALGORITMO DE LA DIVISION

En el Teorema II, Capítulo 12, página 126, ya se dio el algoritmo de la división de polinomios $\alpha(x)$, $\beta(x)$ en x sobre un anillo no conmutativo $\mathscr{R}$ unitario. Allí se supónia que el divisor $\beta(x)$ era mónico. Si el divisor no es mónico, es decir, si el divisor $\beta(x)$ tiene coeficiente dominante $b_n \neq 1$, el teorema es válido solamente si $b_n^{-1} \in \mathscr{R}$.

En el anillo de coeficientes que aquí se considera, toda matriz regular A tiene inversa sobre $\mathscr{F}$; así que el algoritmo puede enunciarse así:

Si $A(\lambda)$ y $B(\lambda)$ son polinomios de matrices (1) y (2) y si B_q es regular, existen entonces pares únicos de polinomios de matrices $Q_1(\lambda), R_1(\lambda)$; $Q_2(\lambda), R_2(\lambda) \in \mathscr{F}[\lambda]$, siendo $R_1(\lambda)$ y $R_2(\lambda)$ bien cero o bien de grado menor que el de $B(\lambda)$, tales que

$$A(\lambda) = Q_1(\lambda) \cdot B(\lambda) + R_1(\lambda) \qquad (4)$$

y

$$A(\lambda) = B(\lambda) \cdot Q_2(\lambda) + R_2(\lambda) \qquad (4')$$

Si en (4) $R_1(\lambda) = 0$, $B(\lambda)$ se dice *divisor a la derecha* de $A(\lambda)$; si en (4') $R_2(\lambda) = 0$, $B(\lambda)$ se dice *divisor a la izquierda* de $A(\lambda)$.

Ejemplo 4:

Dadas

$$A(\lambda) = \begin{bmatrix} \lambda^3 + 3\lambda^2 + 3\lambda & 2\lambda^2 + 5\lambda + 4 \\ \lambda^2 + \lambda - 1 & \lambda^2 + 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \lambda^3 + \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \lambda^2 + \begin{bmatrix} 3 & 5 \\ 1 & 0 \end{bmatrix} \lambda + \begin{bmatrix} 0 & 4 \\ -1 & 1 \end{bmatrix}$$

y

$$B(\lambda) = \begin{bmatrix} \lambda + 1 & 1 \\ \lambda & \lambda + 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \lambda + \begin{bmatrix} 1 & 1 \\ 0 & 2 \end{bmatrix}$$

hallar $Q_1(\lambda), R_1(\lambda)$; $Q_2(\lambda), R_2(\lambda)$ tales que

$$(a) \quad A(\lambda) = Q_1(\lambda) \cdot B(\lambda) + R_1(\lambda), \quad (b) \quad A(\lambda) = B(\lambda) \cdot Q_2(\lambda) + R_2(\lambda)$$

Aquí es $B_1 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq 0$ y $B_1^{-1} = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$

(*a*) Calculamos

$$A(\lambda) - A_3B_1^{-1}\lambda^2B(\lambda) = \begin{bmatrix}2&1\\1&1\end{bmatrix}\lambda^2 + \begin{bmatrix}3&5\\1&0\end{bmatrix}\lambda + \begin{bmatrix}0&4\\-1&1\end{bmatrix} = C(\lambda)$$

$$C(\lambda) - C_2B_1^{-1}\lambda B(\lambda) = \begin{bmatrix}2&2\\1&-2\end{bmatrix}\lambda + \begin{bmatrix}0&4\\-1&1\end{bmatrix} = D(\lambda)$$

$$D(\lambda) - D_1B_1^{-1}B(\lambda) = \begin{bmatrix}0&0\\-4&2\end{bmatrix} = R_1(\lambda)$$

Entonces, $Q_1(\lambda) = (A_3\lambda^2 + C_2\lambda + D_1)B_1^{-1} = \begin{bmatrix}1&0\\0&0\end{bmatrix}\lambda^2 + \begin{bmatrix}1&1\\0&1\end{bmatrix}\lambda + \begin{bmatrix}0&2\\3&-2\end{bmatrix}$

$$= \begin{bmatrix}\lambda^2+\lambda & \lambda+2\\3 & \lambda-2\end{bmatrix}$$

(*b*) Calculamos

$$A(\lambda) - B(\lambda)B_1^{-1}A_3\lambda^2 = \begin{bmatrix}3&2\\3&1\end{bmatrix}\lambda^2 + \begin{bmatrix}3&5\\1&0\end{bmatrix}\lambda + \begin{bmatrix}0&4\\-1&1\end{bmatrix} = E(\lambda)$$

$$E(\lambda) - B(\lambda)B_1^{-1}E_2\lambda = \begin{bmatrix}0&4\\1&2\end{bmatrix}\lambda + \begin{bmatrix}0&4\\-1&1\end{bmatrix} = F(\lambda)$$

$$F(\lambda) - B(\lambda)B_1^{-1}F_1 = \begin{bmatrix}-1&2\\-3&5\end{bmatrix} = R_2(\lambda)$$

Entonces, $Q_2(\lambda) = B_1^{-1}(A_3\lambda^2 + E_2\lambda + F_1) = \begin{bmatrix}1&0\\-1&0\end{bmatrix}\lambda^2 + \begin{bmatrix}3&2\\0&-1\end{bmatrix}\lambda + \begin{bmatrix}0&4\\1&-2\end{bmatrix}$

$$= \begin{bmatrix}\lambda^2+3\lambda & 2\lambda+4\\-\lambda^2+1 & -\lambda-2\end{bmatrix}$$

Véase Problema 5.

Para la matriz cuadrada de orden n $B = [b_{ij}]$ sobre $\mathscr{F}$, defínase su *matriz característica* así:

$$\lambda I - B = \begin{bmatrix}\lambda-b_{11} & -b_{12} & -b_{13} & \dots & -b_{1n}\\ -b_{21} & \lambda-b_{22} & -b_{23} & \dots & -b_{2n}\\ -b_{31} & -b_{32} & \lambda-b_{33} & \dots & -b_{3n}\\ \dots & \dots & \dots & \dots & \dots\\ -b_{n1} & -b_{n2} & -b_{n3} & \dots & \lambda-b_{nn}\end{bmatrix}$$

Con $A(\lambda)$ como en (*1*) y $B(\lambda) = \lambda I - B$, (*4*) y (*4'*) dan

$$A(\lambda) = Q_1(\lambda)\cdot(\lambda I - B) + R_1 \qquad (5)$$

y

$$A(\lambda) = (\lambda I - B)\cdot Q_2(\lambda) + R_2 \qquad (5')$$

en donde los restos R_1 y R_2 no tienen λ. Puede demostrarse además que

$$R_1 = A_R(B) \quad \text{y} \quad R_2 = A_L(B)$$

Ejemplo 5:

Con $A(\lambda) = \begin{bmatrix}\lambda^2 & \lambda-1\\ \lambda+3 & \lambda^2+2\end{bmatrix}$ y $B = \begin{bmatrix}1&2\\2&3\end{bmatrix}$, tenemos $\lambda I - B = \begin{bmatrix}\lambda-1 & -2\\ -2 & \lambda-3\end{bmatrix}$

y

$$A(\lambda) = \begin{bmatrix}\lambda+1 & 3\\3 & \lambda+3\end{bmatrix}(\lambda I - B) + \begin{bmatrix}7&10\\12&17\end{bmatrix} = (\lambda I - B)\begin{bmatrix}\lambda+1 & 3\\3 & \lambda+3\end{bmatrix} + \begin{bmatrix}7&8\\14&17\end{bmatrix}$$

Del Ejemplo 3, los restos son $R_1 = A_R(B) = \begin{bmatrix}7&10\\12&17\end{bmatrix}$ y $R_2 = A_L(B) = \begin{bmatrix}7&8\\14&17\end{bmatrix}$.

RAICES Y VECTORES PROPIOS DE UNA MATRIZ

Estudiemos de nuevo una transformación lineal dada de $V_n(\mathscr{F})$ en sí mismo. Considérese, por ejemplo, la transformación de $V = V_3(R)$ dada por

$$A = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{bmatrix} \quad \text{o} \quad \begin{aligned} \epsilon_1 &\to (2,2,1) \\ \epsilon_2 &\to (1,3,1) \\ \epsilon_3 &\to (1,2,2) \end{aligned}$$

(Recuérdese que en nuestra notación las imágenes de los vectores unitarios ϵ_1, ϵ_2, ϵ_3 del espacio son los vectores fila de A y que la transformación lineal viene dada por

$$V \to V: \quad \xi \to \xi A$$

pues otros escriben los vectores imagen como vectores columna de A. En este caso, la transformación está dada por

$$V \to V: \quad \xi \to A\xi$$

Para la misma matriz A, las dos transformaciones son en general diferentes.)

La imagen de $\xi = (1, 2, 3) \in V$ es

$$\eta = (1,2,3)\begin{bmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{bmatrix} = (7,14,9) \in V$$

vinculada a ξ únicamente por la transformación A. Por otra parte, la imagen de $\xi_1 = (r, 2r, r) \in V$ es $5\xi_1$, esto es, la imagen de cualquier vector del subespacio $V^1 \subset V$, generado por (1, 2, 1), es un vector de V^1. Análogamente, es fácil comprobar que la imagen de cualquier vector del subespacio $V^2 \subset V$, generado por $(1, -1, 0)$, es un vector de V^2 y que la imagen de un vector de $V^3 \subset V$, generado por $(1, 0, -1)$, es un vector de V^3. Asimismo, la imagen de un vector $(s + t, -s, -t)$ del subespacio $V^4 \subset V$, generado por $(1, -1, 0)$ y $(1, 0, -1)$, es un vector del subespacio generado por él mismo. Se deja al lector hacer ver que no ocurre lo mismo ni para el subespacio V^5, generado por (1, 2, 1) y $(1, -1, 0)$, ni para el V^6, generado por (1, 2, 1) y $(1, 0, -1)$.

Resumiendo: La transformación lineal A de $V_3(R)$ aplica un vector del subespacio V^1, generado por (1, 2, 1), en un vector de V^1, y un vector del subespacio V^4, generado por $(1, -1, 0)$ y $(1, 0, -1)$, en un vector del subespacio generado por él mismo. Diremos que un vector no nulo de V^1, o de V^4, es un *vector propio* (*vector invariante* o *autovector*) de la transformación.

En general, sea una transformación lineal de $V = V_n(\mathscr{F})$ referido a la base $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$ dada por una matriz cuadrada de orden n, $A = [a_{ij}]$ sobre $\mathscr{F}$. Todo vector no nulo $\xi = (x_1, x_2, x_3, \ldots, x_n) \in V$ es un vector propio de A siempre que $\xi A = \lambda\xi$, es decir, si

$$\begin{aligned} &(a_{11}x_1 + a_{21}x_2 + \cdots + a_{n1}x_n,\ a_{12}x_1 + a_{22}x_2 + \cdots + a_{n2}x_n,\ \ldots, \\ &\quad a_{1n}x_1 + a_{2n}x_2 + \cdots + a_{nn}x_n) = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n) \end{aligned} \tag{6}$$

para un $\lambda \in \mathscr{F}$.

Utilizaremos ahora (6) para resolver el problema siguiente: Dada A, hallar todos los vectores no nulos ξ tales que $\xi A = \lambda\xi$ con $\lambda \in \mathscr{F}$. Después de igualar las componentes correspondientes en (6), el sistema de ecuaciones resultante se puede escribir como sigue:

$$\begin{cases} (\lambda - a_{11})x_1 - a_{21}x_2 - a_{31}x_3 - \cdots - a_{n1}x_n = 0 \\ -a_{12}x_1 + (\lambda - a_{22})x_2 - a_{32}x_3 - \cdots - a_{n2}x_n = 0 \\ -a_{13}x_1 - a_{23}x_2 + (\lambda - a_{33})x_3 - \cdots - a_{n3}x_n = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ -a_{1n}x_1 - a_{2n}x_2 - a_{3n}x_3 - \cdots + (\lambda - a_{nn})x_n = 0 \end{cases} \tag{7}$$

que, según el Teorema XVIII, Capítulo 14, página 181, tiene solución no trivial si, y solo si, el determinante de la matriz coeficiente

$$\begin{vmatrix} \lambda - a_{11} & -a_{21} & -a_{31} & \dots & -a_{n1} \\ -a_{12} & \lambda - a_{22} & -a_{32} & \dots & -a_{n2} \\ -a_{13} & -a_{23} & \lambda - a_{33} & \dots & -a_{n3} \\ \dots & \dots & \dots & \dots & \dots \\ -a_{1n} & -a_{2n} & -a_{3n} & \dots & \lambda - a_{nn} \end{vmatrix} = |\lambda I - A^T| = 0$$

siendo A^T la transpuesta de A. Ahora bien, $\lambda I - A^T = (\lambda I - A)^T$ (compruébese); luego, por el Teorema XXII, Capítulo 14, $|\lambda I - A^T| = |\lambda I - A|$, el determinante de la matriz característica de A.

Para toda matriz cuadrada de orden n sobre $\mathscr{F}$, $|\lambda I - A^T|$ se llama *determinante característico* de A y su desarrollo, que es un polinomio $\phi(\lambda)$ de grado n, se llama *polinomio característico* de A. Los n ceros $\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_n$ de $\phi(\lambda)$ se llaman *raíces propias* (*raíces latentes* o *autovalores*) de A y, más comúnmente, *valores propios* de A.

Ahora bien, siendo $\phi(\lambda) \in \mathscr{F}[\lambda]$ puede o no tener todos sus ceros en $\mathscr{F}$. (Por ejemplo, el polinomio característico de una matriz cuadrada de orden 2 sobre R tiene ambos ceros en R o bien ninguno en R; el de una matriz cuadrada de orden 3 sobre R tendrá uno o tres ceros en R. Se podrían considerar entonces solamente los subespacios de $V_3(R)$ asociados a los ceros reales, si los hay, o bien ampliar el espacio a $V_3(C)$ y hallar los subespacios asociados a todos los ceros.) Para cualquier raíz o valor propio λ_i, la matriz $\lambda_i I - A^T$ es singular, de modo que el sistema de ecuaciones lineales (7) es linealmente dependiente y existe siempre un vector propio ξ. También $k\xi$ es un vector propio asociado a λ_i para todo escalar k. Además, según el Teorema XVIII, Capítulo 14, página 181, si $\lambda_i I - A^T$ tiene característica r, (7) tiene entonces $n - r$ soluciones linealmente independientes que generan un subespacio de dimensión $n - r$. Todo vector no nulo de este subespacio es un vector propio de A asociado a la raíz o valor propio λ_i.

Ejemplo 6: Determinar los valores propios y los vectores propios asociados de $V_3(R)$, dada $A = \begin{bmatrix} 1 & 1 & 2 \\ 0 & 2 & 2 \\ -1 & 1 & 3 \end{bmatrix}$.

El polinomio característico de A es

$$|\lambda I - A^T| = \begin{vmatrix} \lambda - 1 & 0 & 1 \\ -1 & \lambda - 2 & -1 \\ -2 & -2 & \lambda - 3 \end{vmatrix} = \lambda^3 - 6\lambda^2 + 11\lambda - 6;$$

siendo los valores propios $\lambda_1 = 1$, $\lambda_2 = 2$, $\lambda_3 = 3$; el sistema de ecuaciones lineales (7) es

$$(a) \qquad \begin{cases} (\lambda - 1)x_1 + x_3 = 0 \\ -x_1 + (\lambda - 2)x_2 - x_3 = 0 \\ -2x_1 - 2x_2 + (\lambda - 3)x_3 = 0 \end{cases}$$

Si $\lambda = \lambda_1 = 1$, el sistema (a) se reduce al $\begin{cases} x_1 + x_2 = 0 \\ x_3 = 0 \end{cases}$, que tiene por solución $x_1 = 1$, $x_2 = -1$, $x_3 = 0$. Así, pues, con el valor propio $\lambda_1 = 1$, está asociado el espacio vectorial unidimensional generado por $\xi_1 = (1, -1, 0)$. Todo vector $(k, -k, 0)$, $k \neq 0$ de este subespacio es un vector propio de A.

Si $\lambda = \lambda_2 = 2$, el sistema (a) se reduce al $\begin{cases} x_1 + x_3 = 0 \\ x_1 + 2x_2 = 0 \end{cases}$, cuya solución es $x_1 = 2$, $x_2 = -1$, $x_3 = -2$. Así que con el valor propio $\lambda_2 = 2$, está asociado el espacio vectorial unidimensional generado por $\xi_2 = (2, -1, -2)$, y todo vector $(2k, -k, -2k)$, $k \neq 0$, es un vector propio de A.

Si $\lambda = \lambda_3 = 3$, el sistema (a) se reduce al $\begin{cases} x_1 + x_2 = 0 \\ 2x_1 + x_3 = 0 \end{cases}$, que tiene por solución $x_1 = 1$, $x_2 = -1$, $x_3 = -2$. Así que con el valor propio $\lambda_3 = 3$ está asociado el espacio vectorial unidimensional generado por $\xi_3 = (1, -1, -2)$, y todo vector $(k, -k, -2k)$, $k \neq 0$, es un vector propio de A.

Ejemplo 7: Determinar los valores propios y los vectores propios asociados de $V_3(R)$,

donde $A = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{bmatrix}$.

El polinomio característico es

$$|\lambda I - A^T| = \begin{vmatrix} \lambda-2 & -1 & -1 \\ -2 & \lambda-3 & -2 \\ -1 & -1 & \lambda-2 \end{vmatrix} = \lambda^3 - 7\lambda^2 + 11\lambda - 5;$$

los valores propios son $\lambda_1 = 5$, $\lambda_2 = 1$, $\lambda_3 = 1$; y el sistema de ecuaciones lineales (7) es

$$(a) \qquad \begin{cases} (\lambda-2)x_1 - x_2 - x_3 = 0 \\ -2x_1 + (\lambda-3)x_2 - 2x_3 = 0 \\ -x_1 - x_2 + (\lambda-2)x_3 = 0 \end{cases}$$

Si $\lambda = \lambda_1 = 5$, el sistema (a) se reduce al $\begin{cases} x_1 + x_2 - 3x_3 = 0 \\ x_1 - x_3 = 0 \end{cases}$ que tiene por solución

$x_1 = 1$, $x_2 = 2$, $x_3 = 1$. Así, pues, asociado con $\lambda_1 = 5$ está el espacio vectorial unidimensional generado por $\xi_1 = (1, 2, 1)$. Si $\lambda = \lambda_2 = 1$, el sistema (a) se reduce a $x_1 + x_2 + x_3 = 0$ que tiene $x_1 = 1$, $x_2 = 0$, $x_3 = -1$ y $x_1 = 1$, $x_2 = -1$, $x_3 = 0$ como soluciones linealmente independientes. De modo que asociado con $\lambda_2 = 1$ está el espacio vectorial bidimensional generado por $\xi_2 = (1, 0, -1)$ y $\xi_3 = (1, -1, 0)$.

La matriz del Ejemplo 7 se estudió al comienzo de esta sección. Los Ejemplos 6 y 7, así como el Problema 6, sugieren que con cada valor propio simple está asociado un espacio vectorial unidimensional y que con cada valor propio de multiplicidad $m > 1$ está asociado un espacio vectorial m-dimensional. Lo primero es cierto, pero (véase Problema 7) lo segundo no. No investigaremos aquí este asunto (el lector a quien interese puede consultar cualquier libro de matrices); enunciaremos simplemente

Si λ es una raíz o valor propio de multiplicidad $m \geq 1$ de A, hay entonces un espacio vectorial asociado con λ cuya dimensión es *al menos* 1 y *a lo más* m.

En el Problema 8 demostramos el

Teorema III. Si λ_1, ξ_1; λ_2, ξ_2 son valores propios distintos y vectores propios asociados de una matriz cuadrada de orden n, entonces ξ_1 y ξ_2 son linealmente independientes.

Se deja al lector la demostración del

Teorema IV. La matriz diagonal $D = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ tiene como valores propios $\lambda_1, \lambda_2, \ldots, \lambda_n$ y como vectores propios asociados respectivamente $\epsilon_1, \epsilon_2, \ldots, \epsilon_n$.

MATRICES SEMEJANTES

Dos matrices cuadradas de orden n, A y B sobre $\mathscr{F}$, se dicen *semejantes* sobre $\mathscr{F}$ si existe una matriz regular P sobre $\mathscr{F}$ tal que $B = PAP^{-1}$.

En los Problemas 9 y 10, página 213, demostramos el

Teorema V. Dos matrices semejantes tienen los mismos valores propios.

y el

Teorema VI. Si ζ_i es un vector propio asociado con el valor propio λ_i de $B = PAP^{-1}$, entonces $\xi_i = \zeta_i P$ es un vector propio asociado con el mismo valor propio λ_i de A.

Sea A una matriz cuadrada de orden n sobre $\mathscr{F}$ que tiene por valores propios $\lambda_1, \lambda_2, \ldots, \lambda_n$ semejante a $D = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ y sea P una matriz regular tal que $PAP^{-1} = D$. Según el Teorema IV, ϵ_i es un vector propio asociado con el valor propio λ_i de D, y según el Teorema VI, $\xi_i = \epsilon_i P$ es un vector propio asociado con el mismo valor propio λ_i de A. Ahora bien, $\epsilon_i P$ es el vector fila i-ésimo de P; luego A tiene n vectores propios linealmente independientes $\epsilon_i P$ que forman una base de $V_n(\mathscr{F})$.

Recíprocamente, supóngase que el conjunto S de todos los vectores propios de una matriz cuadrada A de orden n, generan a $V_n(\mathscr{F})$. Entonces, podemos elegir un subconjunto $\{\xi_1, \xi_2, \ldots, \xi_n\}$ de S que es una base de $V_n(\mathscr{F})$. Como cada ξ_i es un vector propio,

$$\xi_1 A = \lambda_1 \xi_1, \quad \xi_2 A = \lambda_2 \xi_2, \quad \ldots, \quad \xi_n A = \lambda_n \xi_n$$

siendo $\lambda_1, \lambda_2, \ldots, \lambda_n$ los valores propios de A. Con $P = \begin{bmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{bmatrix}$, encontramos

$$PA = \begin{bmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \lambda_n \end{bmatrix} P \quad \text{o bien}$$

$$PAP^{-1} = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) = D$$

y A es semejante a D. Hemos demostrado el

Teorema VII. Una matriz cuadrada A de orden n sobre $\mathscr{F}$, que tiene por valores propios $\lambda_1, \lambda_2, \ldots, \lambda_n$ es semejante a $D = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$ si, y solo si, el conjunto S de todos los vectores propios de A generan a $V_n(\mathscr{F})$.

Ejemplo 8: Para la matriz $A = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{bmatrix}$ del Ejemplo 7, tómese $P = \begin{bmatrix} \xi_1 \\ \xi_2 \\ \xi_3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{bmatrix}$.

Entonces, $P^{-1} = \begin{bmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{4} & -\frac{1}{2} \\ \frac{1}{4} & -\frac{3}{4} & \frac{1}{2} \end{bmatrix}$ y

$$PAP^{-1} = \begin{bmatrix} 1 & 2 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 & 2 & 1 \\ 1 & 3 & 1 \\ 1 & 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{4} & -\frac{1}{2} \\ \frac{1}{4} & -\frac{3}{4} & \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 5 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \text{diag}(\lambda_1, \lambda_2, \lambda_3)$$

No toda matriz cuadrada de orden n es semejante a una matriz diagonal. En el Problema 7, página 213, por ejemplo, la condición del Teorema VII no se cumple, ya que el conjunto de los vectores propios solamente genera un subespacio bidimensional de $V_3(R)$.

MATRICES SIMETRICAS REALES

Una matriz cuadrada $A = [a_{ij}]$ de orden n sobre R se dice *simétrica* si $A^T = A$, es decir, si $a_{ij} = a_{ji}$ para todo i y j. La matriz A del Problema 6, página 212, es simétrica; las matrices de los Ejemplos 6 y 7 no lo son.

En el Problema 11, página 214, se demuestra el

Teorema VIII. Los valores propios de una matriz real simétrica son reales.

En el Problema 12, página 214, demostramos el

Teorema IX. Si λ_1, ξ_1; λ_2, ξ_2 son valores propios distintos y vectores propios asociados de una matriz cuadrada de orden n real simétrica, entonces ξ_1 y ξ_2 son mutuamente ortogonales.

Si bien aquí no se dará la demostración, toda matriz real simétrica A es semejante a una matriz diagonal cuyos elementos diagonales son los valores propios de A. Entonces, A tiene n valores propios reales y n vectores propios asociados reales ortogonales entre si

$$\lambda_1, \xi_1;\ \lambda_2, \xi_2;\ \ldots;\ \lambda_n, \xi_n$$

Definiendo ahora $\eta_i = \xi_i/|\xi_i|, \quad (i = 1, 2, \ldots, n),$

A tiene n valores propios reales y n vectores reales unitarios propios asociados ortogonales entre si

$$\lambda_1, \eta_1;\ \lambda_2, \eta_2;\ \ldots;\ \lambda_n, \eta_n$$

Por último, con $S = \begin{bmatrix} \eta_1 \\ \eta_2 \\ \cdot \\ \cdot \\ \cdot \\ \eta_n \end{bmatrix}$, se tiene $SAS^{-1} = \text{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$.

Los vectores $\eta_1, \eta_2, \ldots, \eta_n$ forman una base de $V_n(R)$. Estas bases, que consisten en vectores unitarios ortogonales entre si, se llaman *ortogonales normales* o bien *bases ortonormales*.

MATRICES ORTOGONALES

La matriz S definida en la sección precedente se llama *matriz ortogonal*. Vamos a dar algunas de sus propiedades especiales.

1. Como los vectores fila η_i de S son vectores unitarios ortogonales, es decir, $\eta_i \cdot \eta_j = \begin{cases} 1, & \text{si } i = j \\ 0, & \text{si } i \neq j \end{cases}$ se deduce en seguida que

$$S \cdot S^T = \begin{bmatrix} \eta_1 \\ \eta_2 \\ \cdot \\ \cdot \\ \cdot \\ \eta_n \end{bmatrix} \cdot [\eta_1, \eta_2, \ldots, \eta_n] = \begin{bmatrix} \eta_1 \cdot \eta_1 & \eta_1 \cdot \eta_2 & \cdots & \eta_1 \cdot \eta_n \\ \eta_2 \cdot \eta_1 & \eta_2 \cdot \eta_2 & \cdots & \eta_2 \cdot \eta_n \\ \cdots & \cdots & \cdots & \cdots \\ \eta_n \cdot \eta_1 & \eta_n \cdot \eta_2 & \cdots & \eta_n \cdot \eta_n \end{bmatrix} = I$$

y $S^T = S^{-1}$.

2. Como $S \cdot S^T = S^T \cdot S = I$, los vectores columna de S son también vectores unitarios ortogonales. Así, pues,

Una matriz real H es *ortogonal* si $H \cdot H^T = H^T \cdot H = I$.

3. Considérese la *transformación ortogonal* $Y = XH$ de $V_n(R)$ cuya matriz H es ortogonal y denótese por Y_1, Y_2, respectivamente, las imágenes de $X_1, X_2 \in V_n(R)$. Como

$$Y_1 \cdot Y_2 = Y_1 Y_2^T = (X_1 H)(X_2 H)^T = X_1(H \cdot H^T)X_2^T = X_1 X_2^T = X_1 \cdot X_2,$$

una transformación ortogonal preserva los *productos internos* o *escalares* de vectores.

4. Como $|Y_1| = (Y_1 \cdot Y_2)^{1/2} = (X_1 \cdot X_1)^{1/2} = |X_1|$, una transformación ortogonal preserva la *longitud* de los vectores.

5. Como $\cos\theta' = \dfrac{Y_1 \cdot Y_2}{|Y_1| \cdot |Y_2|} = \dfrac{X_1 \cdot X_2}{|X_1| \cdot |X_2|} \cos\theta$, con $0 \leq \theta, \theta' < \pi$, es $\theta' = \theta$. En particular, si $X_1 \cdot X_2 = 0$, entonces $Y_1 \cdot Y_2 = 0$, es decir, los vectores imagen por una transformación ortogonal de vectores ortogonales, son ortogonales.

Una transformación ortogonal $Y = XH$ (o también la matriz ortogonal H) se dice *propia* o *impropia*, según que $|H| = 1$ o $|H| = -1$.

Ejemplo 9:

Para la matriz A del Problema 6, se tiene

$$\eta_1 = \xi_1/|\xi_1| = (2/\sqrt{6}, -1/\sqrt{6}, -1/\sqrt{6}), \quad \eta_2 = (1/\sqrt{3}, 1/\sqrt{3}, 1/\sqrt{3}), \quad \eta_3 = (0, 1/\sqrt{2}, -1/\sqrt{2})$$

Entonces, con

$$S = \begin{bmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \end{bmatrix} = \begin{bmatrix} 2/\sqrt{6} & -1/\sqrt{6} & -1/\sqrt{6} \\ 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}, \qquad S^{-1} = S^T = \begin{bmatrix} 2/\sqrt{6} & 1/\sqrt{3} & 0 \\ -1/\sqrt{6} & 1/\sqrt{3} & 1/\sqrt{2} \\ -1/\sqrt{6} & 1/\sqrt{3} & -1/\sqrt{2} \end{bmatrix}$$

y tenemos $S \cdot A \cdot S^{-1} = \text{diag}(9, 3, -3)$.

La matriz S del Ejemplo 9 es impropia, es decir, $|S| = -1$. Se puede comprobar fácilmente que si se hubiera utilizado el opuesto de cualquiera de los vectores η_1, η_2, η_3 para formar S, la matriz habría sido propia. De modo que, para toda matriz real simétrica A, siempre puede hallarse una matriz ortogonal propia S tal que $S \cdot A \cdot S^{-1}$ sea una matriz diagonal cuyos elementos diagonales sean los valores propios de A.

CONICAS Y CUADRICAS

Uno de los problemas de la geometría analítica plana y del espacio ordinario es la reducción de las ecuaciones de las cónicas y de las cuádricas a formas canónicas que hagan aparente la naturaleza de estas curvas y superficies.

Sea la ecuación de una cónica referida a ejes coordenados rectangulares OX, OY

$$ax^2 + by^2 + 2cxy + 2dx + 2ey + f = 0 \tag{8}$$

y sea la ecuación de una cuádrica referida a ejes coordenados rectangulares OX, OY y OZ

$$ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz + 2gx + 2hy + 2kz + m = 0 \tag{9}$$

Recuérdese que las reducciones necesarias se efectuan por rotación de ejes para eliminar términos con productos cruzados, y por traslación de ejes para eliminar, cuando ello es posible, términos de grado menor que dos. Aquí nos proponemos esbozar un procedimiento general para tratar cónicas y cuádricas.

Considérese la cónica general de ecuación (8). Sus términos de segundo grado, $ax^2 + by^2 + 2cxy$ se pueden escribir con notación matricial así:

$$ax^2 + by^2 + 2cxy = (x, y) \cdot \begin{bmatrix} a & c \\ c & b \end{bmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = X \cdot E \cdot X^T$$

con $X = (x, y)$. Como E es real y simétrica, existe una matriz ortogonal propia $S = \begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix}$ tal que $S \cdot E \cdot S^{-1} = \text{diag}(\lambda_1, \lambda_2)$, siendo λ_1, η_1; λ_2, η_2 los valores propios y vectores propios asociados unitarios de E. Así que existe una transformación ortogonal propia $X = (x', y')S = X'S$ tal que

$$X'S \cdot E \cdot S^{-1}X'^T = X' \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} X'^T = \lambda_1 x'^2 + \lambda_2 y'^2$$

en donde el término con producto cruzado tiene coeficiente 0.

Sea $S = \begin{bmatrix} \eta_1 \\ \eta_2 \end{bmatrix} = \begin{bmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{bmatrix}$; entonces

$$(x, y) = X = X'S = (x', y')\begin{bmatrix} \eta_{11} & \eta_{12} \\ \eta_{21} & \eta_{22} \end{bmatrix} = [\eta_{11}x' + \eta_{21}y',\ \eta_{12}x' + \eta_{22}y']$$

y tenemos $\begin{cases} x = \eta_{11}x' + \eta_{21}y' \\ y = \eta_{12}x' + \eta_{22}y' \end{cases}$

Esta transformación reduce (8) a

$$\lambda_1 x'^2 + \lambda_2 y'^2 + 2(d\eta_{11} + e\eta_{12})x' + 2(d\eta_{21} + e\eta_{22})y' + f = 0 \qquad (8')$$

que mediante una traslación ha de reducirse a la forma canónica.

Otro procedimiento para obtener (8') es como sigue:

(i) Obténgase la matriz ortogonal propia S.

(ii) Fórmese la asociada de (8)

$$ax^2 + by^2 + 2cxy + 2dxu + 2eyu + fu^2 = (x, y, u) \cdot \begin{bmatrix} a & c & d \\ c & b & e \\ d & e & f \end{bmatrix} \cdot \begin{pmatrix} x \\ y \\ u \end{pmatrix} = \bar{X} \cdot F \cdot \bar{X}^T = 0$$

donde $\bar{X} = (x, y, u)$.

(iii) Utilícese la transformación $\bar{X} = \bar{X}' \begin{bmatrix} S & 0 \\ 0 & 1 \end{bmatrix}$, $\bar{X}' = (x', y', u')$, para obtener

$$\bar{X}' \begin{bmatrix} S & 0 \\ 0 & 1 \end{bmatrix} \cdot F \cdot \begin{bmatrix} S^T & 0 \\ 0 & 1 \end{bmatrix} \bar{X}'^T = 0$$

la asociada de (8').

Ejemplo 10: Identificar la cónica $5x^2 - 2\sqrt{3}\,xy + 7y^2 + 20\sqrt{3}\,x - 44y + 75 = 0$.

Para la matriz $E = \begin{bmatrix} 5 & -\sqrt{3} \\ -\sqrt{3} & 7 \end{bmatrix}$ de los términos de segundo grado, hallamos 4, $(\frac{1}{2}\sqrt{3}, \frac{1}{2})$; 8, $(-\frac{1}{2}, \frac{1}{2}\sqrt{3})$ como valores propios y vectores unitarios asociados propios y formamos $S = \begin{bmatrix} \frac{1}{2}\sqrt{3} & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2}\sqrt{3} \end{bmatrix}$.

Entonces, $\bar{X} = \bar{X}' \begin{bmatrix} S & 0 \\ 0 & 1 \end{bmatrix}$ reduce $\bar{X} \cdot F \cdot \bar{X}^T = \bar{X} \begin{bmatrix} 5 & -\sqrt{3} & 10\sqrt{3} \\ -\sqrt{3} & 7 & -22 \\ 10\sqrt{3} & -22 & 75 \end{bmatrix} \bar{X}^T = 0$ a

$$\bar{X}' \begin{bmatrix} \frac{1}{2}\sqrt{3} & \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2}\sqrt{3} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & -\sqrt{3} & 10\sqrt{3} \\ -\sqrt{3} & 7 & -22 \\ 10\sqrt{3} & -22 & 75 \end{bmatrix} \begin{bmatrix} \frac{1}{2}\sqrt{3} & -\frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2}\sqrt{3} & 0 \\ 0 & 0 & 1 \end{bmatrix} \bar{X}'^T$$

$$= (x', y', u') \begin{bmatrix} 4 & 0 & 4 \\ 0 & 8 & -16\sqrt{3} \\ 4 & -16\sqrt{3} & 75 \end{bmatrix} \cdot \begin{pmatrix} x' \\ y' \\ u' \end{pmatrix} = 4x'^2 + 8y'^2 + 8x'u' - 32\sqrt{3}\,y'u' + 75u'^2 = 0$$

los asociados de $4x'^2 + 8y'^2 + 8x' - 32\sqrt{3}\,y' + 75 = 4(x' + 1)^2 + 8(y' - 2\sqrt{3})^2 - 25 = 0$,

Por la traslación $\begin{cases} x'' = x' + 1 \\ y'' = y' - 2\sqrt{3} \end{cases}$ ésta se convierte en la $4x''^2 + 8''^2 = 25$ y la cónica es una elipse.

Utilizando $\begin{cases} x = \frac{1}{2}\sqrt{3}\,x' - \frac{1}{2}y' \\ y = \frac{1}{2}x' + \frac{1}{2}\sqrt{3}\,y' \end{cases}$ y $\begin{cases} x' = x'' - 1 \\ y' = y'' + 2\sqrt{3} \end{cases}$ se ve fácilmente que, refiriéndonos al sistema de coordenadas original, el nuevo origen está en $O''(-3\sqrt{3}/2, 5/2)$ y que los nuevos ejes $O''X''$ y $O''Y''$ tienen respectivamente las direcciones de los vectores unitarios propios $(\frac{1}{2}\sqrt{3}, \frac{1}{2})$ y $(-\frac{1}{2}, \frac{1}{2}\sqrt{3})$.

Véase Problema 14.

Problemas resueltos

1. Reducir $A(\lambda) = \begin{bmatrix} \lambda & 2\lambda+1 & \lambda+2 \\ \lambda^2+\lambda & 2\lambda^2+2\lambda & \lambda^2+2\lambda \\ \lambda^2-2\lambda & 2\lambda^2-2\lambda-1 & \lambda^2+\lambda-3 \end{bmatrix}$ a forma normal

El máximo común divisor de los elementos de $A(\lambda)$ es 1; hágase $f_1(\lambda) = 1$. Ahora utilícese $K_{21}(-2)$ seguida de K_{12} y procédase luego a eliminar en la primera fila y columna para tener

$$A(\lambda) \sim \begin{bmatrix} 1 & \lambda & \lambda+2 \\ 0 & \lambda^2+\lambda & \lambda^2+2\lambda \\ 2\lambda-1 & \lambda^2-2\lambda & \lambda^2+\lambda-3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda^2+\lambda & \lambda^2+2\lambda \\ 2\lambda-1 & -\lambda^2-\lambda & -\lambda^2-2\lambda-1 \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda^2+\lambda & \lambda^2+2\lambda \\ 0 & -\lambda^2-\lambda & -\lambda^2-2\lambda-1 \end{bmatrix} = B(\lambda)$$

El máximo común divisor de los elementos de la submatriz $\begin{bmatrix} \lambda^2+\lambda & \lambda^2+2\lambda \\ -\lambda^2-\lambda & -\lambda^2-2\lambda-1 \end{bmatrix}$ es 1; hágase $f_2(\lambda) = 1$.

A $B(\lambda)$ aplíquese $H_{23}(1)$ y $K_{23}(-1)$ y luego elimínese en las segundas fila y columna para obtener

$$A(\lambda) \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & \lambda+1 & -\lambda^2-2\lambda-1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda+1 & -\lambda^2-\lambda \end{bmatrix}$$

$$\sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -\lambda^2-\lambda \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda^2+\lambda \end{bmatrix} = N(\lambda)$$

siendo necesario el último paso para que $f_3(\lambda) = \lambda^2 + \lambda$ sea mónico.

2. Reducir (*a*) $A(\lambda) = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda+1 \end{bmatrix}$ y (*b*) $B(\lambda) = \begin{bmatrix} \lambda^3 & 0 & 0 \\ 0 & \lambda^2-\lambda & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix}$ a forma normal

(*a*) El máximo común divisor de los elementos de $A(\lambda)$ es 1. Así,

$$A(\lambda) = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda+1 \end{bmatrix} \sim \begin{bmatrix} \lambda & \lambda+1 \\ 0 & \lambda+1 \end{bmatrix} \sim \begin{bmatrix} -1 & \lambda+1 \\ -\lambda-1 & \lambda+1 \end{bmatrix}$$

$$\sim \begin{bmatrix} -1 & 0 \\ -\lambda-1 & -\lambda^2-\lambda \end{bmatrix} \sim \begin{bmatrix} -1 & 0 \\ 0 & -\lambda^2-\lambda \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & \lambda^2+\lambda \end{bmatrix} = N(\lambda)$$

(*b*) El máximo común divisor de $B(\lambda)$ es λ. Se tiene

$$B(\lambda) = \begin{bmatrix} \lambda^3 & 0 & 0 \\ 0 & \lambda^2-\lambda & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix} \sim \begin{bmatrix} \lambda^3 & \lambda^2-\lambda & 0 \\ 0 & \lambda^2-\lambda & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix} \sim \begin{bmatrix} \lambda^2 & \lambda^2-\lambda & 0 \\ -\lambda^3+\lambda^2 & \lambda^2-\lambda & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix} \sim \begin{bmatrix} \lambda & \lambda^2-\lambda & 0 \\ -\lambda^3+\lambda & \lambda^2-\lambda & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix}$$

$$\sim \begin{bmatrix} \lambda & \lambda^2-\lambda & 0 \\ -\lambda^3 & 0 & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix} \sim \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda^4-\lambda^3 & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix} \sim \begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda^2 & 0 \\ 0 & 0 & \lambda^4-\lambda^3 \end{bmatrix} = N(\lambda)$$

3. Reducir $A(\lambda) = \begin{bmatrix} \lambda-2 & -1 & -1 \\ -2 & \lambda-3 & -2 \\ -1 & -1 & \lambda-2 \end{bmatrix}$ a forma normal

El máximo común divisor de los elementos de $A(\lambda)$ es 1. Utilizamos K_{13} seguida de $K_1(-1)$ y luego eliminamos en las primeras fila y columna para tener

$$A(\lambda) \sim \begin{bmatrix} 1 & -1 & \lambda-2 \\ 2 & \lambda-3 & -2 \\ 2-\lambda & -1 & -1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda-1 & 2-2\lambda \\ 0 & 1-\lambda & \lambda^2-4\lambda+3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & B(\lambda) \end{bmatrix}$$

El máximo común divisor de los elementos de $B(\lambda)$ es $\lambda - 1$; entonces

$$A(\lambda) \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda-1 & 2-2\lambda \\ 0 & 1-\lambda & \lambda^2-4\lambda+3 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda-1 & 0 \\ 0 & 0 & \lambda^2-6\lambda+5 \end{bmatrix} = N(\lambda).$$

4. Expresar $A(\lambda) = \begin{bmatrix} \lambda+2 & \lambda+1 & \lambda+3 \\ \lambda & \lambda & -3\lambda^2+\lambda \\ \lambda^2+2\lambda & \lambda^2+\lambda & 3\lambda^2+5\lambda \end{bmatrix}$ como un polinomio en λ y calcular $A(-2)$.

$A_R(C)$ y $A_L(C)$ si $C = \begin{bmatrix} 1 & 0 & 2 \\ -1 & -1 & -4 \\ -1 & 0 & -2 \end{bmatrix}$.

Obtenemos $$A(\lambda) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -3 \\ 1 & 1 & 3 \end{bmatrix}\lambda^2 + \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 5 \end{bmatrix}\lambda + \begin{bmatrix} 2 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

y $$A(-2) = 4\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -3 \\ 1 & 1 & 3 \end{bmatrix} - 2\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 5 \end{bmatrix} + \begin{bmatrix} 2 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 1 \\ -2 & -2 & -14 \\ 0 & 2 & 2 \end{bmatrix}$$

Como $C^2 = \begin{bmatrix} -1 & 0 & -2 \\ 4 & 1 & 10 \\ 1 & 0 & 2 \end{bmatrix}$, tenemos

$$A_R(C) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -3 \\ 1 & 1 & 3 \end{bmatrix}\begin{bmatrix} -1 & 0 & -2 \\ 4 & 1 & 10 \\ 1 & 0 & 2 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 5 \end{bmatrix}\begin{bmatrix} 1 & 0 & 2 \\ -1 & -1 & -4 \\ -1 & 0 & -2 \end{bmatrix} + \begin{bmatrix} 2 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & -1 \\ -4 & -1 & -10 \\ 2 & 0 & 4 \end{bmatrix}$$

$$A_L(C) = \begin{bmatrix} -1 & 0 & -2 \\ 4 & 1 & 10 \\ 1 & 0 & 2 \end{bmatrix}\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -3 \\ 1 & 1 & 3 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 2 \\ -1 & -1 & -4 \\ -1 & 0 & -2 \end{bmatrix}\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 1 & 5 \end{bmatrix} + \begin{bmatrix} 2 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 2 & 8 \\ 0 & 4 & 5 \\ -3 & -1 & -5 \end{bmatrix}$$

5. Dadas $A(\lambda) = \begin{bmatrix} \lambda^4+\lambda^3+3\lambda^2+\lambda & \lambda^4+\lambda^3+2\lambda^2+\lambda+1 \\ \lambda^3-2\lambda+1 & 2\lambda^3-3\lambda^2-2 \end{bmatrix}$ y $B(\lambda) = \begin{bmatrix} \lambda^2+1 & \lambda^2-\lambda \\ \lambda^2+\lambda & 2\lambda^2+1 \end{bmatrix}$,

hallar $Q_1(\lambda), R_1(\lambda); Q_2(\lambda), R_2(\lambda)$ tales que

(*a*) $A(\lambda) = Q_1(\lambda)\cdot B(\lambda) + R_1(\lambda)$ y (*b*) $A(\lambda) = B(\lambda)\cdot Q_2(\lambda) + R_2(\lambda)$.

Tenemos

$$A(\lambda) = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}\lambda^4 + \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\lambda^3 + \begin{bmatrix} 3 & 2 \\ 0 & -3 \end{bmatrix}\lambda^2 + \begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}\lambda + \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix}$$

$$B(\lambda) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\lambda^2 + \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\lambda + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$B_2 = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \quad \text{y} \quad B_2^{-1} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix}$$

(a) $A(\lambda) - A_4B_2^{-1}\cdot\lambda^2\cdot B(\lambda) = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}\lambda^3 + \begin{bmatrix} 2 & 2 \\ 0 & -3 \end{bmatrix}\lambda^2 + \begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}\lambda + \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} = C(\lambda)$

$C(\lambda) - C_3B_2^{-1}\cdot\lambda\cdot B(\lambda) = \begin{bmatrix} 1 & 2 \\ -1 & -3 \end{bmatrix}\lambda^2 + \begin{bmatrix} 1 & 0 \\ -2 & -1 \end{bmatrix}\lambda + \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} = D(\lambda)$

$D(\lambda) - D_2B_2^{-1}\cdot B(\lambda) = 0 = R_1(\lambda)$

y

$Q_1(\lambda) = (A_4\lambda^2 + C_3\lambda + D_2)B_2^{-1} = \begin{bmatrix} \lambda^2 & \lambda+1 \\ 1 & \lambda-2 \end{bmatrix}$

Aquí, $B(\lambda)$ es divisor a la derecha de $A(\lambda)$.

(b) $A(\lambda) - B(\lambda)\cdot B_2^{-1}A_4\lambda^2 = \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix}\lambda^3 + \begin{bmatrix} 1 & 0 \\ 1 & -2 \end{bmatrix}\lambda^2 + \begin{bmatrix} 1 & 1 \\ -2 & 0 \end{bmatrix}\lambda + \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} = E(\lambda)$

$E(\lambda) - B(\lambda)\cdot B_2^{-1}E_3\lambda = \begin{bmatrix} 0 & 0 \\ 0 & -2 \end{bmatrix}\lambda^2 + \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\lambda + \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} = F(\lambda)$

$F(\lambda) - B(\lambda)\cdot B_2^{-1}F_2 = \begin{bmatrix} 0 & -1 \\ -1 & -2 \end{bmatrix}\lambda + \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & -\lambda-1 \\ -\lambda+1 & -2\lambda \end{bmatrix} = R_2(\lambda)$

y

$Q_2(\lambda) = B_2^{-1}(A_4\lambda^2 + E_3\lambda + F_2) = \begin{bmatrix} 2\lambda^2+\lambda & 2\lambda^2+2 \\ -\lambda^2-\lambda & -\lambda^2-2 \end{bmatrix}$

6. Hallar los valores propios y los vectores propios asociados de $A = \begin{bmatrix} 7 & -2 & -2 \\ -2 & 1 & 4 \\ -2 & 4 & 1 \end{bmatrix}$ sobre R.

El polinomio característico de A es $|\lambda I - A^T| = \begin{vmatrix} \lambda-7 & 2 & 2 \\ 2 & \lambda-1 & -4 \\ 2 & -4 & \lambda-1 \end{vmatrix} = \lambda^3 - 9\lambda^2 - 9\lambda + 81$; los valores propios son $\lambda_1 = 9$, $\lambda_2 = 3$, $\lambda_3 = -3$; y el sistema de ecuaciones lineales (7) es

$$(a) \qquad \begin{cases} (\lambda-7)x_1 + 2x_2 + 2x_3 = 0 \\ 2x_1 + (\lambda-1)x_2 - 4x_3 = 0 \\ 2x_1 - 4x_2 + (\lambda-1)x_3 = 0 \end{cases}$$

Si $\lambda = \lambda_1 = 9$, (a) se reduce a $\begin{cases} x_1 + 2x_2 = 0 \\ x_1 + 2x_3 = 0 \end{cases}$ cuya solución es $x_1 = 2$, $x_2 = -1$, $x_3 = -1$. Así que con $\lambda_1 = 9$ está asociado el espacio vectorial unidimensional generado por $\xi_1 = (2, -1, -1)$.

Si $\lambda = \lambda_2 = 3$, (a) se reduce a $\begin{cases} x_1 - x_3 = 0 \\ x_2 - x_3 = 0 \end{cases}$ que tiene por solución $x_1 = 1$, $x_2 = 1$, $x_3 = 1$. De modo que con $\lambda_2 = 3$ está asociado el espacio vectorial unidimensional generado por $\xi_2 = (1, 1, 1)$.

Si $\lambda = \lambda_3 = -3$, (a) se reduce a $\begin{cases} x_1 = 0 \\ x_2 + x_3 = 0 \end{cases}$ que tiene por solución $x_1 = 0$, $x_2 = 1$, $x_3 = -1$. De modo que con $\lambda_3 = -3$ está asociado el espacio vectorial unidimensional generado por $\xi_3 = (0, 1, -1)$.

7. Hallar los valores propios y los vectores propios asociados de $A = \begin{bmatrix} 0 & -2 & -2 \\ -1 & 1 & 2 \\ -1 & -1 & 2 \end{bmatrix}$ sobre R.

El polinomio característico de A es $|\lambda I - A^T| = \begin{vmatrix} \lambda & 1 & 1 \\ 2 & \lambda - 1 & 1 \\ 2 & -2 & \lambda - 2 \end{vmatrix} = \lambda^3 - 3\lambda^2 + 4$; los valores propios son $\lambda_1 = -1$, $\lambda_2 = 2$, $\lambda_3 = 2$; y el sistema de ecuaciones lineales (7) es

$$(a) \qquad \begin{cases} \lambda x_1 + x_2 + x_3 = 0 \\ 2x_1 + (\lambda - 1)x_2 + x_3 = 0 \\ 2x_1 - 2x_2 + (\lambda - 2)x_3 = 0 \end{cases}$$

Si $\lambda = \lambda_1 = -1$, el sistema (a) se reduce a $\begin{cases} x_1 - x_2 = 0 \\ x_3 = 0 \end{cases}$ cuya solución es $x_1 = 1$, $x_2 = 1$, $x_3 = 0$. De modo que asociado con $\lambda_1 = -1$ está el espacio vectorial unidimensional generado por $\xi_1 = (1, 1, 0)$.

Si $\lambda = \lambda_2 = 2$, el sistema (a) se reduce al $\begin{cases} 3x_1 + x_3 = 0 \\ x_1 - x_2 = 0 \end{cases}$ cuya solución es $x_1 = 1$, $x_2 = 1$, $x_3 = -3$.

Y el espacio vectorial unidimensional asociado a $\lambda_2 = 2$ es generado por $\xi_2 = (1, 1, -3)$.

Nótese que aquí un espacio vectorial de dimensión uno está asociado a una raíz o valor propio doble $\lambda_2 = 2$, mientras que en el Ejemplo 7 con la raíz o valor propio doble estaba asociado un espacio vectorial de dimensión dos.

8. Demostrar: Si λ_1, ξ_1; λ_2, ξ_2 son valores propios distintos y vectores propios asociados a ellos de A, entonces ξ_1 y ξ_2 son linealmente independientes.

Supóngase, por el contrario, ξ_1 y ξ_2 linealmente dependientes; existen entonces escalares a_1 y a_2 ambos no nulos, tales que

$$(i) \qquad a_1\xi_1 + a_2\xi_2 = 0$$

Multiplicando (i) por A y teniendo en cuenta que $\xi_i A = \lambda_i \xi_i$, se tiene

$$(ii) \qquad a_1\xi_1 A + a_2\xi_2 A = a_1\lambda_1\xi_1 + a_2\lambda_2\xi_2 = 0$$

Y entonces (i) y (ii) se cumplen si, y solo si, $\begin{vmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{vmatrix} = 0$. Pero, entonces, $\lambda_1 = \lambda_2$, en contradicción con lo supuesto; luego ξ_1 y ξ_2 son linealmente independientes

9. Demostrar que dos matrices semejantes tienen los mismos valores propios.

Sean A y $B = PAP^{-1}$ matrices semejantes; entonces,

$$\lambda I - B = \lambda I - PAP^{-1} = P\lambda IP^{-1} - PAP^{-1} = P(\lambda I - A)P^{-1}$$

y $$|\lambda I - B| = |P(\lambda I - A)P^{-1}| = |P| \cdot |\lambda I - A| \cdot |P^{-1}| = |\lambda I - A|$$

Con lo que A y B, por tener el mismo polinomio característico, deben tener los mismos valores propios.

10. Demostrar: Si ζ_i es un vector propio asociado con el valor propio λ_i de $B = PAP^{-1}$, entonces $\xi_i = \zeta_i P$ es un vector propio asociado con el mismo valor propio λ_i de A.

Por hipótesis, $\zeta_i B = \lambda_i \zeta_i$ y $BP = (PAP^{-1}) = PA$. Entonces, $\xi_i A = \zeta_i PA = \zeta_i BP = \lambda_i \zeta_i P = \lambda_i \xi_i$ y ξ_i es un vector propio asociado con el vator propio λ_i de A.

11. Demostrar: Los valores propios de una matriz cuadrada de orden n real simétrica son reales.

Sea A una matriz real simétrica y supóngase que $h + ik$ es un valor propio complejo. Ahora bien, $(h + ik)I - A$ es singular como también lo es

$$B = [(h+ik)I - A] \cdot [(h-ik)I - A] = (h^2+k^2)I - 2hA + A^2 = (hI-A)^2 + k^2I$$

Como B es real y singular, existe un vector real no nulo ξ tal que $\xi B = 0$ y, por tanto,

$$\begin{aligned} \xi B\,\xi^T = \xi\{(hI-A)^2 + k^2I\}\xi^T &= \{\xi(hI-A)\}\{(hI-A)^T\xi^T\} + k^2\xi\xi^T \\ &= \eta\cdot\eta + k^2\xi\cdot\xi = 0 \end{aligned}$$

con $\eta = \xi(hI - A)$. Pero $\eta \cdot \eta = 0$, en tanto que por ser ξ real y no nulo, $\xi \cdot \xi > 0$. Luego $k = 0$ y A tiene solamente valores propios reales.

12. Demostrar: Si λ_1, ξ_1; λ_2, ξ_2 son valores propios distintos y vectores propios asociados de una matriz cuadrada de orden n real y simétrica A, ξ_1 y ξ_2 son ortogonales.

Por hipótesis, $\xi_1 A = \lambda_1\xi_1$ y $\xi_2 A = \lambda_2\xi_2$. Entonces,

$$\xi_1 A\,\xi_2^T = \lambda_1\xi_1\xi_2^T \quad \text{y} \quad \xi_2 A\,\xi_1^T = \lambda_2\xi_2\xi_1^T$$

y, tomando transpuestas, $\xi_2 A\,\xi_1^T = \lambda_1\xi_2\xi_1^T$ y $\xi_1 A\,\xi_2^T = \lambda_2\xi_1\xi_2^T$

Ahora bien, $\xi_1 A\,\xi_2^T = \lambda_1\xi_1\xi_2^T = \lambda_2\xi_1\xi_2^T$ y $(\lambda_1 - \lambda_2)\xi_1\xi_2^T = 0$. Como $\lambda_1 - \lambda_2 \neq 0$, se sigue que $\xi_1\xi_2^T = \xi_1 \cdot \xi_2 = 0$ y ξ_1 y ξ_2 son ortogonales.

13. (*a*) Demuéstrese que $\alpha = (2, 1, 3)$ y $\beta = (1, 1, -1)$ son ortogonales.

(*b*) Hallar un vector γ ortogonal a los dos.

(*c*) Utilizar α, β, γ para formar una matriz ortogonal S tal que $|S| = 1$.

(*a*) $\alpha \cdot \beta = 0$; α y β son ortogonales.

(*b*) $\gamma = \alpha \times \beta = (-4, 5, 1)$.

(*c*) Tómese $\rho_1 = \alpha/|\alpha| = (2/\sqrt{14}, 1/\sqrt{14}, 3/\sqrt{14})$, $\rho_2 = \beta/|\beta| = (1/\sqrt{3}, 1/\sqrt{3}, -1/\sqrt{3})$ y $\rho_3 = \gamma/|\gamma| = (-4/\sqrt{42}, 5/\sqrt{42}, 1/\sqrt{42})$. Entonces,

$$\begin{vmatrix} \rho_1 \\ \rho_2 \\ \rho_3 \end{vmatrix} = 1 \quad \text{y} \quad S = \begin{bmatrix} \rho_1 \\ \rho_2 \\ \rho_3 \end{bmatrix} = \begin{bmatrix} 2/\sqrt{14} & 1/\sqrt{14} & 3/\sqrt{14} \\ 1/\sqrt{3} & 1/\sqrt{3} & -1/\sqrt{3} \\ -4/\sqrt{42} & 5/\sqrt{42} & 1/\sqrt{42} \end{bmatrix}$$

14. Identificar la cuádrica

$$3x^2 - 2y^2 - z^2 - 4xy - 8xz - 12yz - 8x - 16y - 34z - 31 = 0$$

Para la matriz $E = \begin{bmatrix} 3 & -2 & -4 \\ -2 & -2 & -6 \\ -4 & -6 & -1 \end{bmatrix}$ de los términos de segundo grado, tómese

$$3, (2/3, -2/3, 1/3);\ 6, (2/3, 1/3, -2/3);\ -9, (1/3, 2/3, 2/3)$$

como valores propios y vectores unitarios propios asociados. Entonces, con $S = \begin{bmatrix} 2/3 & -2/3 & 1/3 \\ 2/3 & 1/3 & -2/3 \\ 1/3 & 2/3 & 2/3 \end{bmatrix}$,

$$\bar{X} = (x, y, z, u) = (x', y', z', u')\begin{bmatrix} S & 0 \\ 0 & 1 \end{bmatrix} = \bar{X}'\begin{bmatrix} S & 0 \\ 0 & 1 \end{bmatrix}$$

reduce
$$\bar{X}\cdot F\cdot \bar{X}^T = \bar{X}\begin{bmatrix} 3 & -2 & -4 & -4 \\ -2 & -2 & -6 & -8 \\ -4 & -6 & -1 & -17 \\ -4 & -8 & -17 & -31 \end{bmatrix}\bar{X}^T$$

a
$$\bar{X}'\begin{bmatrix} 2/3 & -2/3 & 1/3 & 0 \\ 2/3 & 1/3 & -2/3 & 0 \\ 1/3 & 2/3 & 2/3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\cdot\begin{bmatrix} 3 & -2 & -4 & -4 \\ -2 & -2 & -6 & -8 \\ -4 & -6 & -1 & -17 \\ -4 & -8 & -17 & -31 \end{bmatrix}\cdot\begin{bmatrix} 2/3 & 2/3 & 1/3 & 0 \\ -2/3 & 1/3 & 2/3 & 0 \\ 1/3 & -2/3 & 2/3 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}\bar{X}'^T$$

$$= (x', y', z', u')\begin{bmatrix} 3 & 0 & 0 & -3 \\ 0 & 6 & 0 & 6 \\ 0 & 0 & -9 & -18 \\ -3 & 6 & -18 & -31 \end{bmatrix}\begin{pmatrix} x' \\ y' \\ z' \\ u' \end{pmatrix}$$

$$= 3x'^2 + 6y'^2 - 9z'^2 - 6x'u' + 12y'u' - 36z'u' - 31u'^2 = 0$$

el asociado
$$3x'^2 + 6y'^2 - 9z'^2 - 6x' + 12y' - 36z' - 31 = 3(x'-1)^2 + 6(y'+1)^2 - 9(z'+2)^2 - 4 = 0$$

que por la traslación $\begin{cases} x'' = x' - 1 \\ y'' = y' + 1 \\ z'' = z' + 2 \end{cases}$, se convierte en la $3x''^2 + 6y''^2 - 9z''^2 = 4$; la superficie es un hiperboloide de una hoja.

Utilizando $(x, y, z) = (x', y', z')S$ y las ecuaciones de la traslación, se tiene en seguida que, referido al sistema de coordenadas original, el nuevo origen es el punto $(-2/3, -7/3, -1/3)$ y los nuevos ejes tienen la dirección de los vectores propios unitarios $(2/3, -2/3, 1/3)$, $(2/3, 1/3, -2/3)$, $(1/3, 2/3, 2/3)$.

Problemas propuestos

15. Dadas $A(\lambda) = \begin{bmatrix} \lambda^2+\lambda & \lambda+1 \\ \lambda^2+2 & \lambda \end{bmatrix}$ y $B(\lambda) = \begin{bmatrix} \lambda^2 & \lambda^2+\lambda \\ \lambda-1 & \lambda \end{bmatrix}$, hallar

(a) $A(\lambda) + B(\lambda) = \begin{bmatrix} 2\lambda^2+\lambda & \lambda^2+2\lambda+1 \\ \lambda^2+\lambda+1 & 2\lambda \end{bmatrix}$

(b) $A(\lambda) - B(\lambda) = \begin{bmatrix} \lambda & -\lambda^2+1 \\ \lambda^2-\lambda+3 & 0 \end{bmatrix}$

(c) $A(\lambda)\cdot B(\lambda) = \begin{bmatrix} \lambda^4+\lambda^3+\lambda^2-1 & \lambda^4+2\lambda^3+2\lambda^2+\lambda \\ \lambda^4+3\lambda^2-\lambda & \lambda^4+\lambda^3+3\lambda^2+2\lambda \end{bmatrix}$

(d) $B(\lambda)\cdot A(\lambda) = \begin{bmatrix} 2\lambda^4+2\lambda^3+2\lambda^2+2\lambda & 2\lambda^3+2\lambda^2 \\ 2\lambda^2+\lambda & 2\lambda^2-1 \end{bmatrix}$.

16. Para cada una de las siguientes matrices hallar $Q_1(\lambda)$, $R_1(\lambda)$; $Q_2(\lambda)$, $R_2(\lambda)$, siendo $R_1(\lambda)$ y $R_2(\lambda)$ bien 0 o de grado menor que el de $B(\lambda)$ y tales que $A(\lambda) = Q_1(\lambda)\cdot B(\lambda) + R_1(\lambda)$ y $A(\lambda) = B(\lambda)\cdot Q_2(\lambda) + R_2(\lambda)$.

(a) $A(\lambda) = \begin{bmatrix} \lambda^3-2\lambda^2+2\lambda-2 & \lambda^4+\lambda-1 \\ \lambda^4+\lambda^3+\lambda-2 & 2\lambda^2+\lambda-1 \end{bmatrix}$; $B(\lambda) = \begin{bmatrix} \lambda^2+1 & \lambda \\ 1 & \lambda^2+\lambda \end{bmatrix}$

(b) $A(\lambda) = \begin{bmatrix} 2\lambda^2+2\lambda & 2\lambda^2 \\ \lambda^2+\lambda+2 & \lambda^2+2\lambda-1 \end{bmatrix}$; $B(\lambda) = \begin{bmatrix} \lambda & \lambda \\ 1 & \lambda \end{bmatrix}$

(c) $A(\lambda) = \begin{bmatrix} \lambda^3-2\lambda^2+\lambda-3 & 4\lambda^2+2\lambda+3 \\ -2\lambda-2 & \lambda^3+4\lambda^2+6\lambda+3 \end{bmatrix}$; $B(\lambda) = \begin{bmatrix} \lambda-2 & 3 \\ -1 & \lambda+3 \end{bmatrix}$

(d) $A(\lambda) = \begin{bmatrix} \lambda^3-\lambda^2+\lambda+4 & 2\lambda^2+\lambda & \lambda^2+4\lambda-2 \\ 2\lambda & \lambda^3+\lambda^2+2\lambda-1 & 4\lambda^2-2\lambda+1 \\ 3\lambda^2-4\lambda-1 & \lambda^2+\lambda & \lambda^3-2\lambda^2+2\lambda+2 \end{bmatrix}$; $B(\lambda) = \begin{bmatrix} \lambda-1 & 1 & 0 \\ -1 & \lambda+1 & 3 \\ 2 & 0 & \lambda-2 \end{bmatrix}$

Resp. (a) $Q_1(\lambda) = \begin{bmatrix} \lambda-3 & \lambda^2-\lambda \\ \lambda^2+\lambda-1 & -\lambda+2 \end{bmatrix}$; $R_1(\lambda) = \begin{bmatrix} 2\lambda+1 & 4\lambda-1 \\ \lambda-3 & -1 \end{bmatrix}$

$Q_2(\lambda) = \begin{bmatrix} -2 & \lambda^2-1 \\ \lambda^2 & 1 \end{bmatrix}$; $R_2(\lambda) = \begin{bmatrix} 2\lambda & 0 \\ \lambda & 0 \end{bmatrix}$

(b) $Q_1(\lambda) = \begin{bmatrix} 2\lambda+2 & -2 \\ \lambda+1 & 1 \end{bmatrix}$; $R_1(\lambda) = \begin{bmatrix} 2 & 0 \\ 1 & -1 \end{bmatrix}$

$Q_2(\lambda) = \begin{bmatrix} \lambda+2 & \lambda-1 \\ \lambda & \lambda+1 \end{bmatrix}$; $R_2(\lambda) = 0$

(c) $Q_1(\lambda) = \begin{bmatrix} \lambda^2+2 & \lambda-1 \\ \lambda+1 & \lambda^2+\lambda \end{bmatrix}$; $R_1(\lambda) = 0$

$Q_2(\lambda) = \begin{bmatrix} \lambda^2-2 & \lambda+1 \\ \lambda-5 & \lambda^2+\lambda+4 \end{bmatrix}$; $R_2(\lambda) = \begin{bmatrix} 8 & -7 \\ 11 & -8 \end{bmatrix}$

(d) $Q_1(\lambda) = \begin{bmatrix} \lambda^2 & \lambda & \lambda+3 \\ \lambda+1 & \lambda^2+1 & \lambda \\ \lambda-2 & \lambda-1 & \lambda^2-1 \end{bmatrix}$; $R_1(\lambda) = \begin{bmatrix} -2 & 0 & 4 \\ 2 & -3 & -2 \\ -2 & 3 & 3 \end{bmatrix}$

$Q_2(\lambda) = \begin{bmatrix} \lambda^2 & \lambda+2 & \lambda+4 \\ \lambda-2 & \lambda^2 & \lambda-2 \\ \lambda-2 & \lambda+1 & \lambda^2 \end{bmatrix}$; $R_2(\lambda) = \begin{bmatrix} 6 & 2 & 4 \\ 8 & -2 & 7 \\ -5 & -2 & -6 \end{bmatrix}$

17. Reducir a su forma normal:

(a) $\begin{bmatrix} \lambda & 2\lambda & 2\lambda-1 \\ \lambda^2+2\lambda & 2\lambda^2+3\lambda & 2\lambda^2+\lambda-1 \\ \lambda^2-2\lambda & 3\lambda^2-4\lambda & 4\lambda^2-5\lambda+2 \end{bmatrix}$

(b) $\begin{bmatrix} \lambda^2+1 & \lambda^3+\lambda & \lambda^3-\lambda^2 \\ \lambda-1 & \lambda^2+1 & -2\lambda \\ \lambda^2 & \lambda^3 & \lambda^3-\lambda^2+1 \end{bmatrix}$

(c) $\begin{bmatrix} -\lambda & \lambda+1 & \lambda+2 \\ -\lambda^2 & \lambda^2+\lambda-1 & \lambda^2+2\lambda-1 \\ \lambda^2+\lambda+1 & -\lambda^2-2\lambda-1 & -\lambda^2-3\lambda-2 \end{bmatrix}$

(d) $\begin{bmatrix} \lambda^2 & 0 & 0 \\ 0 & \lambda+1 & 0 \\ 0 & 0 & \lambda+1 \end{bmatrix}$

(e) $\begin{bmatrix} \lambda-1 & 3 & -2 \\ -2 & \lambda+1 & 0 \\ 3 & 1 & \lambda+2 \end{bmatrix}$

(f) $\begin{bmatrix} \lambda-2 & 2 & 3 \\ -3 & \lambda+3 & 4 \\ 2 & 0 & \lambda+1 \end{bmatrix}$

Resp. (*a*) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda^2 \end{bmatrix}$ (*c*) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ (*e*) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda^3+2\lambda^2+11\lambda+20 \end{bmatrix}$

(*b*) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda+1 & 0 \\ 0 & 0 & \lambda^3+1 \end{bmatrix}$ (*d*) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & \lambda+1 & 0 \\ 0 & 0 & \lambda^3+\lambda^2 \end{bmatrix}$ (*f*) $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \lambda^3+2\lambda^2-5\lambda-2 \end{bmatrix}$

18. Hallar los valores propios y los vectores propios asociados de cada una de las siguientes matrices A sobre R.

(*a*) $\begin{bmatrix} 1 & -2 \\ -5 & 4 \end{bmatrix}$ (*c*) $\begin{bmatrix} 3 & 1 \\ -1 & 1 \end{bmatrix}$ (*e*) $\begin{bmatrix} 2 & 0 & -1 \\ 0 & 2 & -2 \\ 1 & -1 & 2 \end{bmatrix}$ (*g*) $\begin{bmatrix} 1 & -1 & 0 \\ 1 & 2 & 1 \\ -2 & 1 & -1 \end{bmatrix}$

(*b*) $\begin{bmatrix} 2 & -1 \\ -8 & 4 \end{bmatrix}$ (*d*) $\begin{bmatrix} 1 & -2 \\ -2 & 4 \end{bmatrix}$ (*f*) $\begin{bmatrix} 3 & 2 & 4 \\ 2 & 0 & 2 \\ 4 & 2 & 3 \end{bmatrix}$

Resp. (*a*) $6, (k, -k)$; $-1, (5k, 2k)$ (*e*) $1, (k, -k, -k)$; $2, (2k, -k, 0)$; $3, (k, -k, k)$

(*b*) $0, (4k, k)$; $6, (2k, -k)$ (*f*) $-1, (k, 2l, -k-l)$; $8, (2k, k, 2k)$

(*c*) $2, (k, k)$ (*g*) $1, (3k, 2k, k)$; $2, (k, 3k, k)$; $-1, (k, 0, k)$

(*d*) $0, (2k, k)$; $5, (k, -2k)$

donde $k \neq 0$ y $l \neq 0$.

19. Para una matriz cuadrada A de orden n, demostrar que

(*a*) el término constante de su polinomio característico es $(-1)^n |A|$,

(*b*) el producto de sus valores propios es $|A|$,

(*c*) uno o más de sus valores propios es 0 si, y solo si, $|A| = 0$.

20. Demostrar: El polinomio característico de una matriz cuadrada A de orden n es el producto de los factores invariantes de $\lambda I - A$.

Sugerencia. De $P(\lambda) \cdot (\lambda I - A) \cdot S(\lambda) = \text{diag}\,(f_1(\lambda), f_2(\lambda), \ldots, f_n(\lambda))$ obtener

$$|P(\lambda)| \cdot |S(\lambda)| \cdot \phi(\lambda) = f_1(\lambda) \cdot f_2(\lambda) \ldots f_n(\lambda)$$

con $|P(\lambda)| \cdot |S(\lambda)| = 1$.

21. Para cada una de las siguientes matrices reales simétricas A hallar una matriz ortogonal propia S tal que SAS^{-1} sea diagonal.

(*a*) $\begin{bmatrix} 2 & 2 \\ 2 & -1 \end{bmatrix}$ (*c*) $\begin{bmatrix} 1 & -6 \\ -6 & -4 \end{bmatrix}$ (*e*) $\begin{bmatrix} 3 & -2 & -2 \\ -2 & 8 & -2 \\ -2 & -2 & 3 \end{bmatrix}$ (*g*) $\begin{bmatrix} 3 & -1 & -1 \\ -1 & 2 & 0 \\ -1 & 0 & 2 \end{bmatrix}$

(*b*) $\begin{bmatrix} 4 & -3 \\ -3 & -4 \end{bmatrix}$ (*d*) $\begin{bmatrix} 1 & -2 \\ -2 & 4 \end{bmatrix}$ (*f*) $\begin{bmatrix} 2 & -5 & 0 \\ -5 & -1 & 3 \\ 0 & 3 & -6 \end{bmatrix}$ (*h*) $\begin{bmatrix} 4 & -2 & 4 \\ -2 & 1 & -2 \\ 4 & -2 & 4 \end{bmatrix}$

Resp. (*a*) $\begin{bmatrix} 2/\sqrt{5} & 1/\sqrt{5} \\ -1/\sqrt{5} & 2/\sqrt{5} \end{bmatrix}$ (*c*) $\begin{bmatrix} 3/\sqrt{13} & -2/\sqrt{13} \\ 2/\sqrt{13} & 3/\sqrt{13} \end{bmatrix}$ (*e*) $\begin{bmatrix} 1/3\sqrt{2} & -4/3\sqrt{2} & 1/3\sqrt{2} \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 2/3 & 1/3 & 2/3 \end{bmatrix}$

(*b*) $\begin{bmatrix} 3/\sqrt{10} & -1/\sqrt{10} \\ 1/\sqrt{10} & 3/\sqrt{10} \end{bmatrix}$ (*d*) $\begin{bmatrix} 1/\sqrt{5} & -2/\sqrt{5} \\ 2/\sqrt{5} & 1/\sqrt{5} \end{bmatrix}$ (*f*) $\begin{bmatrix} 5/\sqrt{42} & -4/\sqrt{42} & -1/\sqrt{42} \\ 1/\sqrt{14} & 2/\sqrt{14} & -3/\sqrt{14} \\ 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \end{bmatrix}$

(*g*) $\begin{bmatrix} 2/\sqrt{6} & -1/\sqrt{6} & -1/\sqrt{6} \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \end{bmatrix}$ (*h*) $\begin{bmatrix} 2/3 & -1/3 & 2/3 \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/3\sqrt{2} & 4/3\sqrt{2} & 1/3\sqrt{2} \end{bmatrix}$

22. Identificar las cónicas siguientes:

(*a*) $4x^2 + 24xy + 11y^2 + 16x + 42y + 15 = 0$

(*b*) $9x^2 - 12xy + 4y^2 + 8\sqrt{13}\,x + 12\sqrt{13}\,y + 52 = 0$

(*c*) $3x^2 + 2xy + 3y^2 + 4\sqrt{2}\,x + 12\sqrt{2}\,y - 4 = 0$

Resp. (*a*) Hipérbola, (*b*) Parábola, (*c*) Elipse.

23. Identificar las siguientes cuádricas:

(*a*) $3x^2 + 8y^2 + 8z^2 - 4xy - 4xz - 4yz - 4x - 2y - 4z + 12 = 0$

(*b*) $2x^2 - y^2 - 6z^2 - 10xy + 6yz + 50x - 74y + 42z + 107 = 0$

(*c*) $4x^2 + y^2 + z^2 - 4xy - 4xz + 2yz - 6y + 6z + 2 = 0$

(*d*) $2xy + 2xz + 2yz + 1 = 0$

Resp. (*a*) Paraboloide elíptico, (*b*) Hiperboloide de dos hojas, (*c*) Cilindro parabólico.

24. Sean A con valores propios $\lambda_1, \lambda_2, \ldots, \lambda_n$ y S tales que

$$S \cdot A \cdot S^{-1} = \operatorname{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n) = D$$

Demostrar que $\bar{S} A^T \bar{S}^{-1} = D$ si $\bar{S} = S^{-1}$. Así que toda matriz A semejante a una matriz diagonal es semejante a su transpuesta A^T.

25. Demostrar: Si Q es ortonormal, $Q^T = Q^{-1}$.

26. Demostrar: Toda matriz real cuadrada de orden 2, A, para la cual $|A| < 0$ es semejante a una matriz diagonal.

27. Demostrar por sustitución directa que $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ es un cero de su polinomio característico.

28. ¿En qué condiciones la matriz real $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ tiene

(*a*) valores propios iguales,

(*b*) los valores propios ± 1?

Capítulo 16

Algebras lineales

ALGEBRA LINEAL

Un conjunto $\mathscr{L}$ dotado de las operaciones binarias de adición y multiplicación y de una multiplicación escalar por elementos de un cuerpo conmutativo $\mathscr{F}$, se llama *álgebra lineal* sobre $\mathscr{F}$ si

(i) $\mathscr{L}$ es un espacio vectorial $\mathscr{L}(\mathscr{F})$ sobre $\mathscr{F}$ con respecto a la adición y a la multiplicación escalar.

(ii) La multiplicación es asociativa.

(iii) La multiplicación es distributiva a la izquierda y a la derecha con respecto a la adición.

(iv) $\mathscr{L}$ tiene un elemento neutro multiplicativo (unidad).

(v) $(k\alpha)\beta = \alpha(k\beta) = k(\alpha \cdot \beta)$ para cualesquiera $\alpha, \beta \in \mathscr{L}$ y $k \in \mathscr{F}$.

Ejemplo 1: (*a*) El cuerpo C de los números complejos es un álgebra lineal de dimensión (orden) 2 sobre el cuerpo conmutativo R de los números reales, pues (véase Capítulo 13) $C(R)$ es un espacio vectorial de dimensión 2 y cumple los postulados (ii)-(v).

(*b*) En general, si $\mathscr{L}$ es un cuerpo del que $\mathscr{F}$ es un subcuerpo, $\mathscr{L}$ es un álgebra lineal sobre $\mathscr{F}$.

Ejemplo 2: Es claro que el álgebra de todas las transformaciones lineales del espacio vectorial $V_n(\mathscr{F})$ es un álgebra lineal de orden n^2. Luego el álgebra isomorfa $M_n(\mathscr{F})$ de todas las matrices cuadradas de orden n sobre $\mathscr{F}$ es también un álgebra lineal.

UN ISOMORFISMO

El álgebra lineal del Ejemplo 2 desempeña aquí un papel parecido al del grupo simétrico S_n en teoría de grupos. En el Capítulo 9 se vio que todo grupo abstracto de orden n es isomorfo a un subgrupo de S_n. Ahora vamos a ver que toda álgebra lineal de orden n sobre $\mathscr{F}$ es isomorfa a una subálgebra de $M_n(\mathscr{F})$.

Sea $\mathscr{L}$ un álgebra lineal de orden n sobre $\mathscr{F}$ que tiene por base $\{x_1, x_2, x_3, \ldots, x_n\}$. Con cada $\alpha \in \mathscr{L}$ asóciese la aplicación

$$T_\alpha: \qquad x\,T_\alpha = x \cdot \alpha, \quad x \in \mathscr{L}$$

Por (iii), $$x\,T_\alpha + y\,T_\alpha = x \cdot \alpha + y \cdot \alpha = (x+y)\alpha = (x+y)\,T_\alpha$$

y por (v), $$(kx)\,T_\alpha = (kx)\alpha = k(x \cdot \alpha) = k(x\,T_\alpha)$$

para cualesquiera $x, y \in \mathscr{L}$ y $k \in \mathscr{F}$. Luego $T\alpha$ es una transformación lineal del espacio vectorial $\mathscr{L}(\mathscr{F})$. Además, las transformaciones lineales T_α y T_β asociadas con los elementos distintos α y β de $\mathscr{L}$ son distintas. Pues si $\alpha \neq \beta$, $u \cdot \alpha \neq u \cdot \beta$ con u, la unidad de $\mathscr{L}$, implica $T_\alpha \neq T_\beta$.

Ahora bien, por (iii) y (v),

$$x\,T_\alpha + x\,T_\beta = x \cdot \alpha + x \cdot \beta = x(\alpha+\beta) = x\,T_{\alpha+\beta}$$

$$(x\,T_\alpha)\,T_\beta = (x \cdot \alpha)\beta = x(\alpha \cdot \beta) = x\,T_{\alpha \cdot \beta}$$

y $$(kx)\,T_\alpha = (kx)\alpha = k(x \cdot \alpha) = x \cdot k\alpha = x\,T_{k\alpha}$$

De modo que la aplicación $\alpha \to T_\alpha$ es un isomorfismo de $\mathscr{L}$ sobre una subálgebra del álgebra de todas las transformaciones lineales del espacio vectorial $\mathscr{L}(\mathscr{F})$. Como éste a su vez es isomorfo a una subálgebra de $M_n(\mathscr{F})$, queda demostrado el

Teorema I. Toda álgebra lineal de orden n sobre $\mathscr{F}$ es isomorfa a una subálgebra de $M_n(\mathscr{F})$.

Ejemplo 3: Considérese el álgebra lineal $Q[\sqrt[3]{2}]$ de orden 3 con base $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. Para un elemento cualquiera $a = a_1\,1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4}$ de $Q[\sqrt[3]{2}]$, tenemos

$$\begin{aligned} 1\cdot a &= a_1 1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} \\ \sqrt[3]{2}\cdot a &= 2a_3 1 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} \\ \sqrt[3]{4}\cdot a &= 2a_2 1 + 2a_3\sqrt[3]{2} + a_1\sqrt[3]{4} \end{aligned}$$

Entonces, la aplicación

$$a_1 1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} \to \begin{bmatrix} a_1 & a_2 & a_3 \\ 2a_3 & a_1 & a_2 \\ 2a_2 & 2a_3 & a_1 \end{bmatrix}$$

es un isomorfismo del álgebra lineal $Q[\sqrt[3]{2}]$ sobre el álgebra de todas las matrices de $M_n(Q)$ de la forma $\begin{bmatrix} r & s & t \\ 2t & r & s \\ 2s & 2t & r \end{bmatrix}$.

Véase también Problema 1.

Problemas resueltos

1. Mostrar que $\mathscr{L} = \{a_1\cdot 1 + a_2\alpha + a_3\beta : a_i \in R\}$ con multiplicación definida de modo que 1 es la unidad, $0 = 0\cdot 1 + 0\cdot\alpha + 0\cdot\beta$ es el neutro aditivo, y

(a)

·	α	β
α	α	β
β	0	0

y (b)

·	α	β
α	α	0
β	0	0

son álgebras lineales sobre R.

Podemos verificar simplemente para cada caso que los postulados (i)-(v) se cumplen. En vez de eso es preferible mostrar que en cada caso $\mathscr{L}$ es isomorfa a una subálgebra de $M_3(R)$.

(a) Para cualquier $a = a_1\cdot 1 + a_2\alpha + a_3\beta$, tenemos

$$\begin{aligned} 1\cdot a &= a_1 1 + a_2\alpha + a_3\beta \\ \alpha\cdot a &= (a_1 + a_2)\alpha + a_3\beta \\ \beta\cdot a &= a_1\beta \end{aligned}$$

Luego $\mathscr{L}$ es isomorfa al álgebra de todas las matrices $M_3(R)$ de la forma $\begin{bmatrix} a_1 & a_2 & a_3 \\ 0 & a_1+a_2 & a_3 \\ 0 & 0 & a_1 \end{bmatrix}$ y es un álgebra lineal sobre R.

(b) Para cualquier $a = a_1\cdot 1 + a_2\alpha + a_3\beta$, tenemos

$$\begin{aligned} 1\cdot a &= a_1 1 + a_2\alpha + a_3\beta \\ \alpha\cdot a &= (a_1 + a_2)\alpha \\ \beta\cdot a &= a_1\beta \end{aligned}$$

Luego $\mathscr{L}$ es isomorfa al álgebra de todas las matrices $M_3(R)$ de la forma $\begin{bmatrix} a_1 & a_2 & a_3 \\ 0 & a_1+a_2 & 0 \\ 0 & 0 & a_1 \end{bmatrix}$.

Problemas propuestos

2. Comprobar que cada una de las siguientes, con adición y multiplicación definidas como sobre R, es un álgebra lineal sobre Q.

(*a*) $Q[\sqrt{3}] = \{a1 + b\sqrt{3}: a, b \in Q\}$

(*b*) $\mathscr{L} = \{a1 + b\sqrt{3} + c\sqrt{5} + d\sqrt{15}: a, b, c, d \in Q\}$

3. Demostrar que el álgebra lineal $\mathscr{L} = Q[\sqrt{t}]$, no siendo $t \in N$ un cuadrado perfecto, es isomorfa al álgebra de las matrices de $M_2(Q)$ de la forma $\begin{bmatrix} a & b \\ tb & a \end{bmatrix}$.

4. Demostrar que el álgebra lineal C sobre R es isomorfa al álgebra de todas las matrices de $M_2(R)$ de la forma $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

5. Demostrar que cada una de las siguientes es un álgebra lineal sobre R. Obtener el conjunto de matrices isomorfas de cada una.

(*a*) $\mathscr{L} = \{a1 + b\alpha + c\alpha^2: a, b, c \in R\}$, siendo $G = \{\alpha, \alpha^2, \alpha^3 = 1\}$ el grupo cíclico de orden 3.

(*b*) $\mathscr{L} = \{a_1 1 + a_2 x + a_3 y: a_i \in R\}$, con multiplicación definida de modo que 1 es la unidad, $0 = 0 \cdot 1 + 0 \cdot x + 0 \cdot y$ es el neutro aditivo y

·	x	y
x	1	y
y	y	0

(*c*) $\mathscr{Q} = \{a_1 + a_2 i + a_3 j + a_4 k: a_i \in R\}$ con tabla de multiplicación

·	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

Resp. (*a*) $\begin{bmatrix} a & b & c \\ c & a & b \\ b & c & a \end{bmatrix}$ (*b*) $\begin{bmatrix} a_1 & a_2 & a_3 \\ a_2 & a_1 & a_3 \\ 0 & 0 & (a_1 + a_2) \end{bmatrix}$ (*c*) $\begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ -a_2 & a_1 & -a_4 & a_3 \\ -a_3 & a_4 & a_1 & -a_2 \\ -a_4 & -a_3 & a_2 & a_1 \end{bmatrix}$

Capítulo 17

Algebras boolianas

ALGEBRA BOOLIANA

Un conjunto $\mathscr{B}$ sobre el cual se han definido operaciones binarias $\cup$ y $\cap$, se llama *álgebra booliana* si se cumplen los postulados siguientes:

(i) $\cup$ y $\cap$ son conmutativas.

(ii) $\mathscr{B}$ contiene un elemento neutro 0 con respecto a $\cup$ y un elemento neutro 1 con respecto a $\cap$.

(iii) Cada operación es distributiva con respecto a la otra, es decir, para cualesquiera $a, b, c \in \mathscr{B}$

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$$

y

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$$

(iv) Para todo $a \in \mathscr{B}$ existe un $a' \in \mathscr{B}$ tal que

$$a \cup a' = 1 \qquad \text{y} \qquad a \cap a' = 0$$

Con frecuencia se emplean los símbolos más familiares $+$ y $\cdot$ en vez de $\cup$ y $\cap$. Utilizaremos los últimos porque si el conjunto vacio $\varnothing$ se denotará ahora por 0 y el conjunto universal U por 1, es claro que las identidades 1.9-1.9′, 1.4-1.4′, 1.10-1.10′, 1.7-1.7′, cuya validez se demostró en el Capitulo 1 para el álgebra de los subconjuntos de un conjunto dado, serian precisamente los postulados (i)-(iv) para un álgebra booliana. Lo primero que hemos de hacer, pues, será demostrar, sin recurrir a los subconjuntos de un conjunto dado, que las identidades 1.1, 1.2-1.2′, 1.5-1.5′, 1.6-1.6′, 1.8-1.8′, 1.11-1.11′ del Capítulo 1 son también válidas para toda álgebra booliana, es decir, que estas identidades son consecuencias de los postulados (i)-(iv). Es de notar que hay completa simetria en los postulados con respecto a las operaciones $\cup$ y $\cap$ y también en las identidades de (iv). Se deduce, por tanto, para toda álgebra booliana, el

Principio de dualidad. Todo teorema deducible de los postulados (i)-(iv) de un álgebra booliana sigue siendo válido si se intercambian los símbolos de operación $\cup$ y $\cap$ y los elementos neutros 0 y 1 entre sí.

Consecuencia del principio de dualidad es que basta con demostrar solo uno de los enunciados de cada pareja de duales.

Ejemplo 1: Demostrar: Para todo $a \in \mathscr{B}$,

$$a \cup a = a \qquad \text{y} \qquad a \cap a = a \tag{1}$$

(Véase 1.6-1.6′, Capítulo 1, página 5.)

Utilizando sucesivamente (ii), (iv), (iii), (iv), (ii):

$$a \cup a = (a \cup a) \cap 1 = (a \cup a) \cap (a \cup a') = a \cup (a \cap a') = a \cup 0 = a$$

Ejemplo 2: Demostrar: Para todo $a \in \mathscr{B}$,

$$a \cup 1 = 1 \qquad \text{y} \qquad a \cap 0 = 0 \tag{2}$$

(Véase 1.5-1.5′, Capitulo 1, página 5.)

Utilizando sucesivamente (ii), (iv), (iii), (ii), (iv):

$$a \cap 0 = 0 \cup (a \cap 0) = (a \cap a') \cup (a \cap 0) = a \cap (a' \cup 0) = a \cap a' = 0$$

Ejemplo 3: Demostrar: Para cualesquiera, $a, b \in \mathscr{B}$,

$$a \cup (a \cap b) = a \qquad \text{y} \qquad a \cap (a \cup b) = a \tag{3}$$

Utilizando sucesivamente (ii), (iii), (2), (ii):

$$a \cup (a \cap b) = (a \cap 1) \cup (a \cap b) = a \cap (1 \cup b) = a \cap 1 = a$$

Vèanse también Problemas 1-4.

FUNCIONES BOOLIANAS

Sea $\mathscr{B} = \{a, b, c, \ldots\}$ un álgebra booliana. Por *constante* se entenderá cualquier simbolo, como 0 y 1, que represente un elemento particular de $\mathscr{B}$; por *variable* se entenderá un símbolo que represente un elemento cualquiera de $\mathscr{B}$. Si en la expresión $x' \cup (y \cap z)$ remplazamos $\cup$ por $+$ y $\cap$ por $\cdot$ para obtener $x' + y \cdot z$, parece natural llamar a x' y $y \cap z$ *monomios* y toda la expresión $x' \cup (y \cap z)$ *polinomio*.

Toda expresión como $x \cup x'$, $a \cap b'$, $[a \cap (b \cup c')] \cup (a' \cap b' \cap c)$ que consiste en combinaciones por $\cup$ e $\cap$ de un número finito de elementos de un álgebra booliana $\mathscr{B}$ se dirá *función booliana*. El número de variables en una función es el número de letras distintas que aparezcan, tomándose una letra con tilde como si no la tuviera. Asi, $x \cup x'$ es una función de una variable, x, pero $a \cap b'$ es una función de dos variables, a y b.

En el álgebra ordinaria toda función entera de varias variables se puede expresar siempre como un polinomio (incluso 0), pero no siempre se puede expresar como producto de factores lineales. En cambio, en el álgebra booliana las funciones boolianas se pueden expresar en general en forma polinómica (incluso 0 y 1), es decir, como unión de intersecciones distintas, y en forma factorizada, es decir, como intersección de uniones distintas.

Ejemplo 4:

Simplificar

(a) $(x \cap y) \cup [(x \cup y') \cap y]'$, (b) $[(x \cup y') \cap (x \cap y' \cap z)']'$, (c) $\{[(x' \cap y')' \cup z] \cap (x \cup z)\}'$

(a) $(x \cap y) \cup [(x \cup y') \cap y]' = (x \cap y) \cup [(x \cup y')' \cup y'] = (x \cap y) \cup [(x' \cap y) \cup y']$

$= (x \cap y) \cup [(x' \cup y') \cap (y \cup y')] = (x \cap y) \cup [(x' \cup y') \cap 1]$

$= (x \cap y) \cup (x' \cup y') = (x \cap y) \cup (x \cap y)' = 1$

(b) $[(x \cup y') \cap (x \cap y' \cap z)']' = (x \cup y')' \cup [(x \cap y' \cap z)']'$

$= (x' \cap y) \cup (x \cap y' \cap z)$, una unión de intersecciones

$[(x \cup y') \cap (x \cap y' \cap z)']' = (x' \cap y) \cup (x \cap y' \cap z)$

$= (x' \cup x) \cap (x' \cup y') \cap (x' \cup z) \cap (x \cup y) \cap (y \cup y') \cap (y \cup z)$

$= 1 \cap (x' \cup y') \cap (x' \cup z) \cap (x \cup y) \cap 1 \cap (y \cup z)$

$= (x \cup y) \cap (y \cup z) \cap (x' \cup z) \cap (x' \cup y')$, una intersección de uniones

(c) $\{[(x' \cap y')' \cup z] \cap (x \cup z)\}' = [(x' \cap y')' \cup z]' \cup (x \cup z)'$

$= (x' \cap y' \cap z') \cup (x' \cap z') = x' \cap z'$ (por el Ejemplo 3)

Vèase también Problema 5.

Como (vèase Problema 15, página 234) existe un álgebra booliana con los solos elementos 0 y 1, cualquier identidad se puede comprobar dando a las variables los valores 0 y 1 de todas las maneras posibles.

Ejemplo 5: Para comprobar la identidad propuesta (véase Ejemplo 4(a))

$$(x \cap y) \cup [(x \cup y') \cap y]' = 1$$

se forma la siguiente Tabla 17-1.

x	y	$a = x \cap y$	$x \cup y'$	$b = (x \cup y') \cap y$	$a \cup b'$
1	1	1	1	1	1
1	0	0	1	0	1
0	1	0	0	0	1
0	0	0	1	0	1

Tabla 17-1

FORMAS NORMALES

La función booliana en tres variables del Ejemplo 4(*b*) cuando se expresa como unión de intersecciones $(x' \cap y) \cup (x \cap y' \cap z)$ contiene un término en el cual solo aparecen dos de las variables. En la sección siguiente veremos que a veces hay buenas razones para sustituir esta expresión por una menos simple en que cada término tenga todas las variables. Como la variable z falta en el primer término de la expresión anterior se obtiene la forma requerida, llamada *forma canónica* o *forma normal disyuntiva* de la función dada, de la manera siguiente:

$$\begin{aligned}(x' \cap y) \cup (x \cap y' \cap z) &= (x' \cap y \cap 1) \cup (x \cap y' \cap z) \\ &= [(x' \cap y) \cap (z \cup z')] \cup (x \cap y' \cap z) \\ &= (x' \cap y \cap z) \cup (x' \cap y \cap z') \cup (x \cap y' \cap z)\end{aligned}$$

Véase también Problema 6.

Es fácil mostrar que la forma canónica de una función booliana en tres variables puede tener 2^3 términos distintos a lo más. Pues si x, y, z son las variables, se obtiene un término eligiendo x o x', y o y', z o z' y formando su intersección. En general, la forma canónica de una función booliana en n variables puede contener a lo más 2^n términos distintos. La forma canónica que contiene todos estos 2^n términos se dice *forma canónica completa* o *forma normal disyuntiva completa en n variables*.

La forma canónica completa en n variables es idénticamente 1, cosa que se muestra para el caso $n = 3$ en el Problema 7, página 231; pero el caso general se puede demostrar por inducción. Se sigue de inmediato que el complemento F' de una función booliana F expresada en forma canónica es la unión de todos los términos de la forma canónica completa que no aparecen en forma canónica de F. Por ejemplo, si $F = (x \cap y) \cup (x' \cap y) \cup (x' \cap y')$, $F' = (x \cap y')$.

En los Problemas 8 y 9 se demuestran

Teorema I. Si en la forma canónica completa en n variables se da a cada variable el valor 0 o el 1, solo un término tendrá el valor 1 y todos los demás tendrán el valor 0.

y

Teorema II. Dos funciones booleanas son iguales si, y solo si, sus formas canónicas respectivas son idénticas, es decir, constan de los mismos términos.

La función booliana en tres variables del Ejemplo 4(*b*), expresada como intersección de uniones en que cada unión contiene todas las variables, es

$$\begin{aligned}&(x \cup y) \cap (y \cup z) \cap (x' \cup z) \cap (x' \cup y') \\ &\quad = [(x \cup y) \cup (z \cap z')] \cap [(y \cup z) \cup (x \cap x')] \cap [(x' \cup z) \cup (y \cap y')] \cap [(x' \cup y') \cup (z \cap z')] \\ &\quad = (x \cup y \cup z) \cap (x \cup y \cup z') \cap (x' \cup y \cup z) \cap (x' \cup y' \cup z) \cap (x' \cup y' \cup z')\end{aligned}$$

Expresión que se llama *forma canónica dual* o *forma normal conjuntiva* de la función. Nótese que no es la dual de la forma canónica de aquella función.

El dual [illegible] la forma canónica de una función booliana es un enunciado válido sobre [illegible] de esa función. (Nótese que el dual de *término* es *factor*.) La forma canónica [illegible] en n variables puede tener a lo más 2^n factores distintos. La forma canónica [illegible] estos factores se llama *forma canónica dual completa* o *forma normal conjuntiva* [illegible] y su valor es idénticamente 0. El complemento F' de una función booliana F [illegible] canónica dual es la intersección de todos los factores de la forma canónica dual [illegible] que no aparecen en la forma canónica dual de F. Se tiene, asimismo,

Teorema I. [illegible] dual completa en n variables cada variable toma el valor 0 ó 1, [illegible] valdrá 0 y todos los demás valdrán 1;

y

Teorema II. [illegible] son iguales si, y solo si, sus formas canónicas duales respectivas son idénticas, es decir, consisten en los mismos factores.

En la sección que sigue emplearemos estos teoremas para determinar la función booliana cuando se dan sus valores para todas las maneras posibles de dar valores 0 y 1 a las variables.

CAMBIO DE FORMA DE UNA FUNCION BOOLIANA

Denótese por $F(x, y, z)$ la función booliana cuyos valores para todas las posibles maneras de dar el valor 0 ó 1 a las variables vienen dados por la Tabla 17-2.

La demostración del Teorema I sugiere que los términos que aparecen en la forma canónica de $F(x, y, z)$ son precisamente los de la forma canónica completa en tres variables que tienen valor 1 cuando $F(x, y, z) = 1$. Por ejemplo, la primera fila de la tabla da $x \cap y \cap z$ como término y la tercera fila dice que $x \cap y' \cap z$ es otro término. Así,

x	y	z	$F(x, y, z)$
1	1	1	1
1	1	0	0
1	0	1	1
0	1	1	0
1	0	0	0
0	1	0	0
0	0	1	1
0	0	0	1

Tabla 17-2

$$\begin{aligned} F(x, y, z) &= (x \cap y \cap z) \cup (x \cap y' \cap z) \cup (x' \cap y' \cap z) \cup (x' \cap y' \cap z') \\ &= (x \cap z) \cup (x' \cap y') \end{aligned}$$

Análogamente, los factores que aparecen en la forma canónica dual de $F(x, y, z)$ son precisamente los de la forma canónica dual completa que tienen el valor 0 cuando $F(x, y, z) = 0$. Tenemos

$$\begin{aligned} F(x, y, z) &= (x' \cup y' \cup z) \cap (x \cup y' \cup z') \cap (x' \cup y \cup z) \cap (x \cup y' \cup z) \\ &= (x' \cup z) \cap (x \cup y') \end{aligned}$$

Véase Problema 10.

Si se da una función booliana F en forma canónica o canónica dual, para pasar a la otra forma se emplean sucesivamente las dos reglas para hallar el complemento; si bien el orden en que esto se haga puede ser cualquiera, a veces un cierto orden exige menos cálculo que el otro.

Ejemplo 6: Hallar la forma canónica dual de

$$F = (x \cap y \cap z') \cup (x \cap y' \cap z) \cup (x \cap y' \cap z') \cup (x' \cap y \cap z) \cup (x' \cap y' \cap z')$$

Aquí es $$F' = (x \cap y \cap z) \cup (x' \cap y' \cap z) \cup (x' \cap y \cap z')$$

(la unión de todos los términos de la forma canónica completa que no aparecen en F) y

$$F = (F')' = (x \cup y \cup z') \cap (x \cup y' \cup z) \cap (x' \cup y' \cup z') \quad \text{(por el Problema 4)}$$

Véase también Problema 11.

El procedimiento para cambiar de la forma canónica a la forma canónica dual y viceversa puede utilizarse también ventajosamente para simplificar ciertas funciones booleanas.

Ejemplo 7: Simplificar: $F = [(y \cap z') \cup (y' \cap z)] \cap [(x' \cap y) \cup (x' \cap z) \cup (x \cap y' \cap z')]$

Hágase $F_1 = (y \cap z') \cup (y' \cap z)$ and $F_2 = (x' \cap y) \cup (x' \cap z) \cup (x \cap y' \cap z')$.

Entonces, $F_1 = (x \cap y \cap z') \cup (x' \cap y \cap z') \cup (x \cap y' \cap z) \cup (x' \cap y' \cap z)$

$F_1' = (x' \cap y \cap z) \cup (x' \cap y' \cap z') \cup (x \cap y \cap z) \cup (x \cap y' \cap z')$

y $F_1 = (x \cup y' \cup z') \cap (x \cup y \cup z) \cap (x' \cup y' \cup z') \cap (x' \cup y \cup z)$

Asimismo, $F_2 = (x' \cap y \cap z) \cup (x' \cap y \cap z') \cup (x' \cap y' \cap z) \cup (x \cap y' \cap z')$

$F_2' = (x' \cap y' \cap z') \cup (x \cap y \cap z) \cup (x \cap y' \cap z) \cup (x \cap y \cap z')$

y $F_2 = (x \cup y \cup z) \cap (x' \cup y' \cup z') \cap (x' \cup y \cup z') \cap (x' \cup y' \cup z)$

Con lo que $F = F_1 \cap F_2$

$= (x \cup y \cup z) \cap (x \cup y' \cup z') \cap (x' \cup y \cup z) \cap (x' \cup y \cup z')$
$\cap (x' \cup y' \cup z) \cap (x' \cup y' \cup z')$

Pero entonces $F' = (x \cup y' \cup z) \cap (x \cup y \cup z')$

y $F = (x' \cap y \cap z') \cup (x' \cap y' \cap z) = x' \cap [(y \cap z') \cup (y' \cap z)]$

RELACION DE ORDEN DE UN ALGEBRA BOOLIANA

Sean $U = \{a, b, c\}$ y $S = \{\varnothing, A, B, C, D, E, F, U\}$ con $A = \{a\}$, $B = \{b\}$, $C = \{c\}$, $D = \{a, b\}$, $E = \{a, c\}$, $F = \{b, c\}$. La relación $\subseteq$ definida en el Capitulo 1, aplicada a S, satisface las leyes siguientes:

Para cualquier $X, Y, Z \in S$,

(*a*) $X \subseteq X$

(*b*) Si $X \subseteq Y$ y $Y \subseteq X$, $X = Y$.

(*c*) Si $X \subseteq Y$ y $Y \subseteq Z$, $X \subseteq Z$.

(*d*) Si $X \subseteq Y$ y $X \subseteq Z$, $X \subseteq (Y \cap Z)$.

(*e*) Si $X \subseteq Y$, $X \subseteq (Y \cup Z)$.

(*f*) $X \subseteq Y$ si, y solo si, $Y' \subseteq X'$.

(*g*) $X \subseteq Y$ si, y solo si, $X \cup Y = Y$ o la equivalente $X \cap Y' = \varnothing$.

Las tres primeras leyes dicen (véase Capítulo 2) que $\subseteq$ efectúa un orden parcial en S que se ilustra por

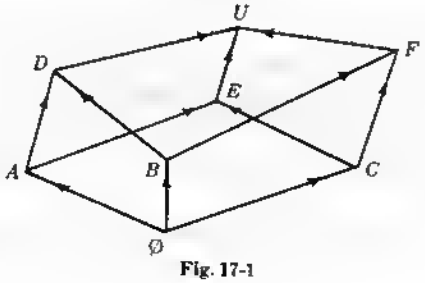


Fig. 17-1

Vamos a definir ahora la relación $\subseteq$ (léase «bajo») en un álgebra booliana $\mathscr{B}$ por

$$a \subseteq b \text{ si, y solo si, } a \cup b = b \text{ o su equivalente } a \cap b' = 0$$

para cualesquiera $a, b \in \mathscr{B}$. (Nótese que esto no es más que otro enunciado de (g) en función de los elementos de $\mathscr{B}$.) De lo que se sigue de inmediato

(a_1) $a \subseteq a$
(b_1) Si $a \subseteq b$ y $b \subseteq a$, $a = b$.
(c_1) Si $a \subseteq b$ y $b \subseteq c$, $a \subseteq c$.

así que $\subseteq$ define un orden parcial en $\mathscr{B}$. Se deja al lector demostrar que

(d_1) Si $a \subseteq b$ y $a \subseteq c$, entonces $a \subseteq (b \cap c)$.
(e_1) Si $a \subseteq b$, entonces $a \subseteq (b \cup c)$ para todo $c \in \mathscr{B}$.
(f_1) $a \subseteq b$ si, y solo si, $b' \subseteq a'$.

En el Problema 12 demostramos el

Teorema III. Para cualesquiera $a, b \in \mathscr{B}$, $a \cup b$ es el extremo superior y $a \cap b$ es el extremo inferior de a y b.

De lo que se deduce fácilmente

Teorema IV. $0 \subseteq b \subseteq 1$ para todo $b \in \mathscr{B}$.

ALGEBRA DE REDES ELECTRICAS

El álgebra de las redes eléctricas es un ejemplo interesante y de mucha importancia del álgebra booliana (véase Problema 15) de los dos elementos 0 y 1. Aquí nos limitaremos a estudiar el tipo más sencillo de redes, que es una red con solo interruptores. La red más simple de esta clase consiste en un hilo con un solo interruptor r:

Al cerrar el interruptor, con lo que la corriente fluye por el hilo, damos el valor 1 a r; si el interruptor está abierto y no fluye corriente por el hilo, damos el valor 0 a r. Asimismo, daremos el valor 1 ó 0 a toda red según que la corriente fluya o no por ella. En este caso sencillo la red tiene valor 1 si, y solo si, r tiene valor 1 y la red tiene valor 0 si, y solo si, r tiene valor 0.

Considérese ahora una red que consiste en dos interruptores r y s. Si se conectan en *serie*:

Fig. 17-2

es claro que la red tiene valor 1 si, y solo si, r y s tienen valor 1, en tanto que la red tiene valor 0 para todo otro valor 0 ó 1 dado a r y s. Así que esta red se puede representar por la función $F = F(r, s)$ que sigue la Tabla 17-3. Se halla fácilmente $F = r \cap s$. Si se conectan en *paralelo*:

r	s	F
1	1	1
1	0	0
0	1	0
0	0	0

Tabla 17-3

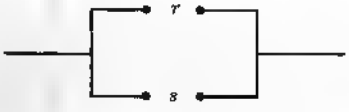


Fig. 17-3

es claro que la red tendrá valor 1 si, y solo si, al menos uno de los r y s tiene valor 1, y la red tendrá valor 0 si, y solo si, ambos r y s tienen valor 0. Esta red se puede representar por la función $F = F(r, s)$ que sigue la Tabla 17-4. Encontramos fácilmente $F = r \cup s$. Para las varias redes con tres interruptores, vèase Problema 13.

r	s	F
1	1	1
1	0	1
0	1	1
0	0	0

Tabla 17-4

Empleando más interruptores, pueden componerse redes de naturaleza más complicada; por ejemplo,

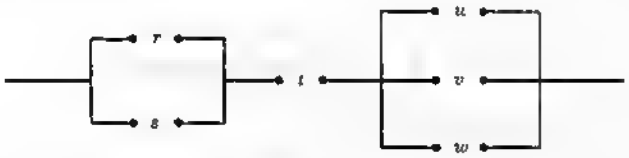


Fig. 17-4

La función correspondiente a esta red consiste en la intersección de tres factores:

$$(r \cup s) \cap t \cap (u \cup v \cup w)$$

Hasta aqui todos los interruptores de una red se han supuesto actuar independientemente unos de otros. Dos o más interruptores pueden, no obstante, estar conectados de modo que (a) se abren y cierran simultáneamente o (b) el cierre (apertura) de uno abra (cierre) todos los demás. En el caso (a) denotaremos todos los interruptores por la misma letra y en el caso (b) denotaremos uno de los interruptores por r, por ejemplo, y todos los otros por r'. En este caso, toda letra con tilde tiene valor 0 si la letra no tildada tiene valor 1 y viceversa. Asi la red

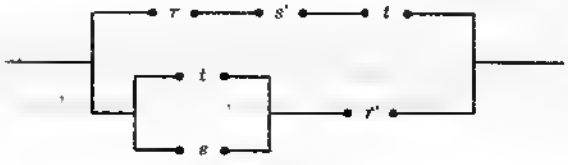


Fig. 17-5

consiste en tres pares de interruptores: un par, en que cada interruptor está denotado por t, abre y cierra simultáneamente, y los otros dos pares, con los interruptores denotados por r, r' y s, s', son tales que en cada par el cierre de un interruptor abre el otro. La función correspondiente es básicamente una unión de dos términos cada uno con las tres variables. Para el hilo superior tenemos $r \cap s' \cap t$ y para el inferior $(t \cup s) \cap r'$. Así que la función que corresponde a la red es

$$F = (r \cap s' \cap t) \cup [(t \cup s) \cap r']$$

y la tabla que da los valores (propiedades de cierre) de la función es

r	s	t	$r \cap s' \cap t$	$(t \cup s) \cap r'$	F
1	1	1	0	0	0
1	1	0	0	0	0
1	0	1	1	0	1
0	1	1	0	1	1
1	0	0	0	0	0
0	1	0	0	1	1
0	0	1	0	1	1
0	0	0	0	0	0

Tabla 17-5

Es claro que la corriente fluirá por la red solamente en los siguientes casos: (1) r y t cerrados, s abierto; (2) s y t cerrados, r abierto; (3) s cerrado, r y t abiertos; (4) t cerrado, r y s abiertos.

Para un análisis más detenido de las redes serie-paralelo será útil saber que el álgebra de tales redes es un álgebra booliana. En términos de una red dada, el problema es éste: Supóngase que F es la función (de interrupción) asociada a la red y supóngase que mediante las leyes del álgebra booliana esta función se cambia en su forma a G asociada con una red distinta. ¿Son intercambiables las dos redes? O, en otras palabras, ¿tienen las mismas propiedades de cierre (la misma tabla)? Para decidir esto, consideremos primero las Tablas 17-3 y 17-4 junto con sus redes asociadas y funciones asociadas $r \cap s$ y $r \cup s$ respectivamente. Al formar estas tablas hemos comprobado que los postulados (i), (ii), (iv) para un álgebra booliana valen también para un álgebra de redes. Para el caso del postulado (iii) considérense las redes

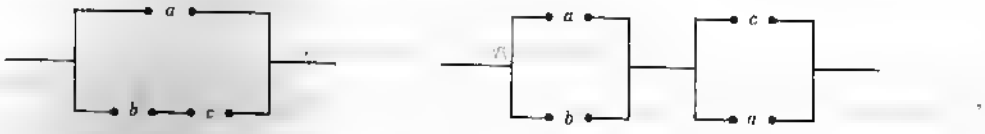


Fig. 17-6

que corresponden a la entidad booliana $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$. Es claro entonces por la tabla de propiedades de cierre

a	b	c	$a \cup (b \cap c)$	$(a \cup b) \cap (a \cup c)$
1	1	1	1	1
1	1	0	1	1
1	0	1	1	1
0	1	1	1	1
1	0	0	1	1
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0

Tabla 17-6

que las redes son intercambiables.

Se deja al lector el examen del caso de la identidad booliana

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$$

y la conclusión de que el álgebra de redes es un álgebra booliana

SIMPLIFICACION DE REDES

Supóngase ahora que las tres primeras y la última columna de la Tabla 17-5 son dadas y que se pide diseñar una red que tenga las propiedades de cierre dadas. Mediante las filas en que $F = 1$, obtenemos

$$F = (r \cap s' \cap t) \cup (r' \cap s \cap t) \cup (r' \cap s \cap t') \cup (r' \cap s' \cap t) = (r' \cap s) \cup (s' \cap t)$$

Como ésta no es la función (red) de la cual se originó el cálculo de la tabla, la red de la Fig. 17-5 es innecesariamente complicada y puede cambiarse por la red más sencilla de la Figura 17-7.

Fig. 17-7

Nota. El que uno de los interruptores de la Fig. 17-7 esté denotado por r', no habiendo interruptor denotado por r, no tiene aquí importancia. Si le queda al lector alguna duda en esto, intercambie r y r' en la Fig. 17-5 y obtenga $F = (r \cap s) \cup (s' \cap t)$ con el diagrama

Fig. 17-8

Véase Problema 14.

Problemas resueltos

1. Demostrar: $\cup$ y $\cap$ son asociativos, es decir, que para cualesquiera $a, b, c \in \mathscr{B}$

$$(a \cup b) \cup c = a \cup (b \cup c) \qquad \text{y} \qquad (a \cap b) \cap c = a \cap (b \cap c) \tag{4}$$

(Véase 1.8-1.8′, Capítulo 1, página 5.)

Sean $x = (a \cap b) \cap c$ y $y = a \cap (b \cap c)$. Vamos a demostrar que $x = y$. Por (iii) y (3),

$$\begin{aligned} a \cup x &= a \cup [(a \cap b) \cap c] = [a \cup (a \cap b)] \cap (a \cup c) \\ &= a \cap (a \cup c) = a = a \cup [a \cap (b \cap c)] = a \cup y \end{aligned}$$

y

$$\begin{aligned} a' \cup x &= a' \cup [(a \cap b) \cap c] = [a' \cup (a \cap b)] \cap (a' \cup c) = [(a' \cup a) \cap (a' \cup b)] \cap (a' \cup c) \\ &= [1 \cap (a' \cup b)] \cap (a' \cup c) = (a' \cup b) \cap (a' \cup c) = a' \cup (b \cap c) \\ &= (a' \cup a) \cap [a' \cup (b \cap c)] = a' \cup [a \cap (b \cap c)] = a' \cup y \end{aligned}$$

Luego

$$\begin{aligned} (a \cup x) \cap (a' \cup x) &= (a \cup y) \cap (a' \cup y) \\ (a \cap a') \cup x &= (a \cap a') \cup y \end{aligned}$$

y

$$x = y$$

Se deja al lector mostrar que, en consecuencia, se pueden insertar paréntesis a voluntad en $a_1 \cup a_2 \cup \cdots \cup a_n$ y $a_1 \cap a_2 \cap \cdots \cap a_n$.

2. Demostrar: Para todo $a \in \mathscr{B}$, en elemento a' definido en (iv) es único.

Supóngase lo contrario, es decir, que para todo $a \in \mathscr{B}$ existan dos elementos $a', a'' \in \mathscr{B}$ tales que

$$\begin{aligned} a \cup a' &= 1 \\ a \cup a'' &= 1 \end{aligned} \qquad \text{y} \qquad \begin{aligned} a \cap a' &= 0 \\ a \cap a'' &= 0 \end{aligned}$$

Entonces,

$$a' = 1 \cap a' = (a \cup a'') \cap a' = (a \cap a') \cup (a'' \cap a')$$

$$= (a \cap a'') \cup (a'' \cap a') = a'' \cap (a \cup a') = a'' \cap 1 = a''$$

y a' es único.

3. Demostrar: Para cualesquiera $a, b \in \mathscr{B}$

$$(a \cup b)' = a' \cap b' \qquad \text{y} \qquad (a \cap b)' = a' \cup b' \tag{5}$$

(Véase 1.11-1.11′, Capítulo 1, página 5.)

Como según el Problema 2 existe para todo $x \in \mathscr{B}$ un único x' tal que $x \cup x' = 1$ y $x \cap x' = 0$, solo necesitamos comprobar que

$$\begin{aligned} (a \cup b) \cup (a' \cap b') &= [(a \cup b) \cup a'] \cap [(a \cup b) \cup b'] = [(a \cup a') \cup b] \cap [a \cup (b \cup b')] \\ &= (1 \cup b) \cap (a \cup 1) = 1 \cap 1 = 1 \end{aligned}$$

y que (lo dejamos al lector) $(a \cup b) \cap (a' \cap b') = 0$

Utilizando los resultados del Problema 2, se sigue fácilmente que

$$(a_1 \cup a_2 \cup \cdots \cup a_n)' = a_1' \cap a_2' \cap \cdots \cap a_n'$$

y

$$(a_1 \cap a_2 \cap \cdots \cap a_n)' = a_1' \cup a_2' \cup \cdots \cup a_n'$$

4. Demostrar: $(a')' = a$ para todo $a \in \mathscr{B}$. (Véase 1.1, Capitulo 1, página 5.)

$$(a')' = 1 \cap (a')' = (a \cup a') \cap (a')' = [a \cap (a')'] \cup [a' \cap (a')'] = [a \cap (a')'] \cup 0$$
$$= 0 \cup [a \cap (a')'] = (a \cap a') \cup [a \cap (a')'] = a \cap [a' \cup (a')'] = a \cap 1 = a$$

5. Simplificar: $[x \cup (x' \cup y)'] \cap [x \cup (y' \cap z')']$.

$$[x \cup (x' \cup y)'] \cap [x \cup (y' \cap z')'] = [x \cup (x \cap y')] \cap [x \cup (y \cup z)] = x \cap [x \cup (y \cup z)] = x$$

6. Obtener la forma canónica de $[x \cup (x' \cup y)'] \cap [x \cup (y' \cap z')']$.

Utilizando la identidad del Problema 5,

$$[x \cup (x' \cup y)'] \cap [x \cup (y' \cap z')'] = x = x \cap (y \cup y') \cap (x \cup z')$$
$$= (x \cap y \cap z) \cup (x \cap y' \cap z) \cup (x \cap y \cap z') \cup (x \cap y' \cap z')$$

7. Demostrar: La forma canónica completa en 3 variables es idénticamente 1.

Primero, mostramos que la forma canónica completa en 2 variables

$$(x \cap y) \cup (x \cap y') \cup (x' \cap y) \cup (x' \cap y') = [(x \cap y) \cup (x \cap y')] \cup [(x' \cap y) \cup (x' \cap y')]$$
$$= [x \cap (y \cup y')] \cup [x' \cap (y \cup y')]$$
$$= (x \cup x') \cap (y \cup y') = 1 \cap 1 = 1$$

Entonces, la forma canónica completa en 3 variables

$$[(x \cap y \cap z) \cup (x \cap y \cap z')] \cup [(x \cap y' \cap z) \cup (x \cap y' \cap z')]$$
$$\cup [(x' \cap y \cap z) \cup (x' \cap y \cap z')] \cup [(x' \cap y' \cap z) \cup (x' \cap y' \cap x')]$$
$$= [(x \cap y) \cup (x \cap y') \cup (x' \cap y) \cup (x' \cap y')] \cap (z \cup z') = 1 \cap 1 = 1$$

8. Demostrar: Si en la forma canónica completa en n variables, a cada variable se le da arbitrariamente el valor 0 ó 1, entonces solo un término tendrá valor 1 y todos los otros tendrán valor 0.

Sean dados los valores a las variables $x_1, x_2, \ldots, x_n$. El término cuyo valor es 1 contiene x_1 si x_1 tiene el valor 1 asignado o bien x_1' si a x_1 se ha dado el valor 0, x_2 si x_2 tiene valor 1 o x_2' si x_2 tiene el valor 0, ..., x_n si x_n tiene valor 1 o x_n' si x_n tiene valor 0. Todo otro término de la forma canónica completa tendrá, pues, 0 al menos como un factor y, por tanto, tendrá 0 como valor.

9. Demostrar: Dos funciones boolianas son iguales si, y solo si, sus formas canónicas respectivas son idénticas, es decir, consisten en los mismos términos.

Es claro que dos funciones son iguales si sus formas canónicas consisten en los mismos términos. Recíprocamente, si las dos funciones son iguales deben tener el mismo valor para cada una de las 2^n posibilidades de dar valor 0 ó 1 a las variables. Además, cada una de las 2^n posibilidades para las cuales la función tiene valor 1 determina un término de la forma canónica de esa función. Luego las dos formas normales contienen los mismos términos.

10. Hallar la función booliana F definida por

x	y	z	F
1	1	1	0
1	1	0	1
1	0	1	1
0	1	1	0
1	0	0	1
0	1	0	1
0	0	1	0
0	0	0	1

Tabla 17-7

Es claro que la forma canónica de F tendrá 5 términos y la forma canónica dual tendrá 3 factores. Emplearemos la última forma. Entonces,

$$F = (x' \cup y' \cup z') \cap (x \cup y' \cup z') \cap (x \cup y \cup z')$$
$$= (y' \cup z') \cap (x \cup y \cup z') = [y' \cap (x \cup y)] \cup z' = (x \cap y') \cup z'$$

11. Hallar la forma canónica de $F = (x \cup y \cup z) \cap (x' \cup y' \cup z)$.

Aquí $$F' = (x' \cap y' \cap z') \cup (x \cap y \cap z')$$

(por la identidad del Problema 3) y

$$F = (F')' = (x \cap y \cap z) \cup (x \cap y' \cap z) \cup (x \cap y' \cap z') \cup (x' \cap y \cap z) \cup (x' \cap y' \cap z) \cup (x' \cap y \cap z')$$

(la unión de los términos de la forma canónica completa que no aparecen en F').

12. Demostrar: Para cualesquiera $a, b \in \mathscr{B}$, $a \cup b$ es el extremo superior y $a \cap b$ es el extremo inferior de a y b.

Que $a \cup b$ es un mayorante de a y b resulta de

$$a \cup (a \cup b) = a \cup b = b \cup (a \cup b)$$

Sea c cualquier otro mayorante de a y b. Entonces, $a \subseteq c$ y $b \subseteq c$, de modo que $a \cup c = c$ y $b \cup c = c$. Ahora bien,

$$(a \cup b) \cup c = a \cup (b \cup c) = a \cup c = c$$

Así que $(a \cup b) \subseteq c$ y $a \cup b$ es el mínimo mayorante o extremo superior como se pedía.

Análogamente, $a \cap b$ es un minorante de a y b, pues

$$(a \cap b) \cup a = a \quad \text{y} \quad (a \cap b) \cup b = b$$

Sea c cualquier otro minorante de a y b. Entonces, $c \subseteq a$ y $c \subseteq b$, de modo que $c \cup a = a$ y $c \cup b = b$. Ahora bien,

$$c \cup (a \cap b) = (c \cup a) \cap (c \cup b) = a \cap b$$

Así que $c \subseteq (a \cap b)$ y $a \cap b$ es el máximo minorante o extremo inferior como se pedía.

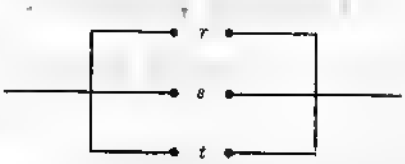
13. Estudiar las posibles redes de tres interruptores r, s, t.

Hay cuatro casos:

(i) Los interruptores están en serie. El diagrama es

y la función es $r \cap s \cap t$.

(ii) Los interruptores están en paralelo. El diagrama es



y la función es $r \cup s \cup t$.

(iii) La combinación serie-paralelo

con función $r \cap (s \cup t)$.

(iv) La combinación serie-paralelo

con función $r \cup (s \cap t)$.

14. Si es posible, remplazar la red

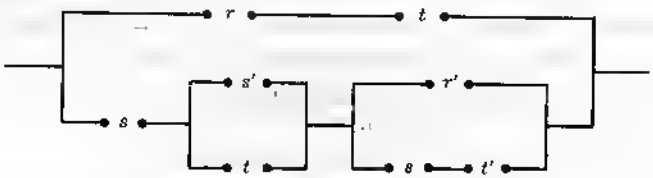


Fig. 17-9(*a*)

por una más simple.

La función booliana para la red dada es

$$\begin{aligned} F &= (r \cap t) \cup \{s \cap (s' \cup t) \cap [r' \cup (s \cap t')]\} \\ &= (r \cap t) \cup \{s \cap [(s' \cup t) \cap (r' \cup t')]\} \\ &= (r \cap t) \cup [r' \cap (s \cap t)] = (r \cup s) \cap t \end{aligned}$$

La red más simple es

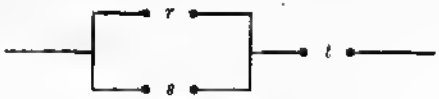


Fig. 17-9(*b*)

Problemas propuestos

15. Mostrar que el conjunto $\{0, 1\}$ junto con las operaciones definidas en

$\cup$	0	1
0	0	1
1	1	1

y

$\cap$	0	1
0	0	0
1	0	1

es un álgebra booliana.

16. Mostrar que el conjunto $\{a, b, c, d\}$ con las operaciones definidas en

$\cup$	a	b	c	d
a	a	b	c	d
b	b	b	d	d
c	c	d	c	d
d	d	d	d	d

y

$\cap$	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	a	c	c
d	a	b	c	d

es un álgebra booliana.

17. Mostrar que el álgebra booliana del Problema 16 es isomorfa al álgebra de todos los subconjuntos de un conjunto de dos elementos.

18. ¿Por qué no hay álgebra booliana que tenga solamente tres elementos distintos?

19. Sea S un subconjunto de N, y para cualesquiera $a, b \in S$ definase $a \cup b$ y $a \cap b$, respectivamente, como el mínimo común múltiplo y el máximo común divisor de a y b. Mostrar que
(*a*) $\mathscr{B}$ es álgebra booliana si $S = \{1, 2, 3, 6, 7, 14, 21, 42\}$.
(*b*) $\mathscr{B}$ no es álgebra booliana si $S = \{1, 2, 3, 4, 6, 8, 12, 24\}$.

20. Mostrar que $a \cup (a \cap b) = a \cap (a \cup b)$ sin utilizar el Ejemplo 3, página 223. Establecer la dual de la identidad y demostrarla.

21. Demostrar: Para cualesquiera $a, b \in \mathscr{B}$, $a \cup (a' \cap b) = a \cup b$. Establecer la dual y demostrarla.

22. Obtener las identidades del Ejemplo 1, página 222, haciendo $b = a$ en las identidades del Problema 21.

23. Obtener como en el Problema 22 las identidades del Ejemplo 2, página 222.

24. Demostrar: $0' = 1$ y $1' = 0$. (Véase 1.2-1.2', Capítulo 1, página 5.)
Sugerencia. Hágase $a = 0$ y $b = 1$ en la identidad del Problema 21.

25. Demostrar: $(a \cap b') \cup (b \cap a') = (a \cup b) \cap (a' \cup b')$. Escribir la dual.

26. Demostrar: $(a \cup b) \cap (b \cup c) \cap (c \cup a) = (a \cap b) \cup (b \cap c) \cup (c \cap a)$. ¿Cuál es la dual?

27. Demostrar: Si $a \cup x = b \cup x$ y $a \cup x' = b \cup x'$ es $a = b$.
Sugerencia. Considérese $(a \cup x) \cap (a \cup x') = (b \cup x) \cap (b \cup x')$.

28. Establecer la dual del Problema 27 y demostrarla.

29. Demostrar: Si $a \cap b = a \cap c$ y $a \cup b = a \cup c$ para cualesquiera $a, b, c \in \mathscr{B}$, entonces $b = c$.

30. Simplificar
(*a*) $(a \cup b) \cap a' \cap b'$
(*b*) $(a \cap b \cap c) \cup a' \cup b' \cup c'$
(*c*) $(a \cap b) \cup [c \cap (a' \cup b')]$
(*d*) $[a \cup (a' \cap b)] \cap [b \cup (b \cap c)]$
(*e*) $[(x' \cap y')' \cup z] \cap (x \cup y')'$
(*f*) $(a \cup b') \cap (a' \cup b) \cap (a' \cup b')$
(*g*) $[(a \cup b) \cap (c \cup b')] \cup [b \cap (a' \cup c')]$

Resp. (*a*) 0, (*b*) 1, (*c*) $(a \cap b) \cup c$, (*d*) b, (*e*) $x' \cap y$, (*f*) $a' \cap b'$, (*g*) $a \cup b$

31. Demostrar:
$$(a \cup b) \cap (a' \cup c) = (a' \cap b) \cup (a \cap c) \cup (b \cap c)$$
$$= (a \cup b) \cap (a' \cup c) \cap (b \cup c) = (a \cap c) \cup (a' \cap b)$$

32. Hallar a simple vista el complemento de cada una de las siguientes expresiones, de dos maneras:
(*a*) $(x \cap y) \cup (x \cap y')$
(*b*) $(x \cap y' \cap z) \cup (x' \cap y \cap z')$
(*c*) $(x \cup y' \cup z) \cap (x \cup y \cup z') \cap (x \cup y' \cup z')$
(*d*) $(x \cup y' \cup z) \cap (x' \cup y \cup z)$

33. Expresar lo que sigue en forma canónica y en forma canónica dual en tres variables:

(*a*) $x' \cup y'$, (*b*) $(x \cap y') \cup (x' \cap y)$, (*c*) $(x \cup y) \cap (x' \cup z')$, (*d*) $x \cap z$, (*e*) $x \cap (y' \cup z)$

Respuesta parcial.

(a) $(x \cap y' \cap z) \cup (x \cap y' \cap z') \cup (x' \cap y \cap z) \cup (x' \cap y' \cap z) \cup (x' \cap y \cap z') \cup (x' \cap y' \cap z')$
(b) $(x \cup y \cup z) \cap (x \cup y \cup z') \cap (x' \cup y' \cup z) \cap (x' \cup y' \cup z')$
(c) $(x \cap y \cap z') \cup (x \cap y' \cap z') \cup (x' \cap y \cap z) \cup (x' \cap y \cap z')$
(d) $(x \cup y \cup z) \cap (x \cup y' \cup z) \cap (x \cup y \cup z') \cap (x \cup y' \cup z') \cap (x' \cup y \cup z) \cap (x' \cup y' \cup z)$
(e) $(x \cup y \cup z) \cap (x \cup y' \cup z) \cap (x \cup y \cup z') \cap (x \cup y' \cup z') \cap (x' \cup y' \cup z)$

34. Expresar en forma canónica y forma canónica dual en el mínimo número de variables:

(a) $x \cup (x' \cap y)$
(b) $[x \cap (y \cup z)] \cup [x \cap (y \cup z')]$
(c) $(x \cup y \cup z) \cap [(x \cap y) \cup (x' \cap z)]$
(d) $(x \cap y \cap z) \cup [(x \cup y) \cap (x \cup z)]$
(e) $(x \cup y) \cap (x \cup z') \cap (x' \cup y') \cap (x' \cup z)$
(f) $(x \cap y) \cup (x \cap z') \cup (x' \cap z)$

Respuesta parcial.

(a) $(x \cap y) \cup (x \cap y') \cup (x' \cap y)$
(b) $(x \cup y) \cap (x \cup y')$
(c) $(x \cap y \cap z) \cup (x \cap y \cap z') \cup (x' \cap y \cap z) \cup (x' \cap y' \cap z)$
(d) $(x \cup y \cup z) \cap (x \cup y \cup z') \cap (x \cup y' \cup z)$
(e) $(x \cap y' \cap z) \cup (x' \cap y \cap z')$
(f) $(x \cup y \cup z) \cap (x' \cup y \cup z') \cap (x \cup y' \cup z)$

35. Escribir el término de la forma canónica completa en x, y, z, que tiene valor 1 cuando:

(a) $x = z = 1$, $y = 1$; (b) $x = y = 1$, $z = 0$; (c) $x = 0$, $y = z = 1$.

Resp. (a) $x' \cap y \cap z'$, (b) $x \cap y \cap z'$

36. Escribir el término de la forma canónica completa en x, y, z, w, que tiene el valor 1 cuando:

(a) $x = y = 1$, $z = w = 0$; (b) $x = y = w = 0$, $z = 1$; (c) $x = 0$, $y = z = w = 1$.

Resp. (a) $x \cap y \cap z' \cap w'$, (c) $x' \cap y \cap z \cap w$

37. Escribir el factor de la forma canónica dual completa en x, y, z, que tiene valor 0 cuando:

(a) $x = z = 1$, $y = 1$; (b) $x = y = 1$, $z = 0$; (c) $x = 0$, $y = z = 1$.

Resp. (a) $x \cup y' \cup z$, (b) $x' \cup y' \cup z$

38. Escribir el factor de la forma canónica dual completa en x, y, z, w, que tiene valor 0 cuando:

(a) $x = y = 1$, $z = w = 0$; (b) $x = y = w = 0$, $z = 1$; (c) $x = 0$, $y = z = w = 1$.

Resp. (a) $x' \cup y' \cup z \cup w$, (c) $x \cup y' \cup z' \cup w'$

39. Escribir la función en tres variables cuyo valor es 1
(a) si y sólo si dos de las variables son 1 y la otra es 0,
(b) si y sólo si más de una variable es 1.

Resp. (a) $(x \cap y \cap z') \cup (x \cap y' \cap z) \cup (x' \cap y \cap z)$, (b) $[x \cap (y \cup z)] \cup (y \cap z)$

40. Escribir la función en tres variables cuyo valor es 0
(a) si y sólo si dos de las variables son 0 y la otra es 1,
(b) si y sólo si más de una variable es 0.

Resp. Las mismas de el Problema 39.

41. Obtener en la forma más simple las funciones booleanas $F_1, F_2, \ldots, F_8$ definidas como sigue:

x	y	z	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
1	1	1	0	1	0	1	1	1	0	1
1	1	0	1	0	1	0	0	0	0	0
1	0	1	0	1	1	1	1	1	1	1
1	0	1	0	1	1	1	0	0	0	1
0	1	0	1	0	0	0	1	0	1	0
0	1	0	0	1	1	1	0	0	0	0
0	0	1	0	1	1	1	1	1	1	1
0	0	0	1	1	1	0	0	1	1	0

Resp. $F_1 = xy' \cap z'$, $F_3 = x' \cup (y' \cap z) \cup (y \cap z')$, $F_5 = (x \cup z) \cap [y' \cup (x \cap z)]$, $F_7 = y'$

42. Mostrar que F_7 y F_8 del Problema 41 se pueden hallar a simple vista.

43. Demostrar: (d_1) Si $a \subseteq b$ y $a \subseteq c$, entonces $a \subseteq (b \cap c)$.
(e_1) Si $a \subseteq b$ entonces $a \subseteq (b \cup c)$ para todo $c \in \mathscr{B}$.
(f_1) $a \subseteq b$ si, y solo si, $b' \subseteq a'$.

44. Demostrar: Si $a, b \in \mathscr{B}$ tales que $a \subseteq b$, entonces, para todo $c \in \mathscr{B}$, $a \cup (b \cap c) = b \cap (a \cup c)$.

45. Demostrar: Para todo $b \in \mathscr{B}$, $0 \subseteq b \subseteq 1$.

46. Construir un diagrama parecido a la Fig. 17-1 para el álgebra booliana de todos los subconjuntos de $B = \{a, b, c, d\}$.

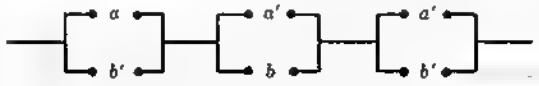
47. Hacer el diagrama de las redes representadas por $a \cup (a' \cap b')$ y $a \cup b$ y hacer ver con tablas que tienen las mismas propiedades de cierre.

48. Hacer diagramas de las redes (i) $(a \cup b) \cap a' \cap b'$ y (ii) $(a \cap b \cap c) \cup (a' \cup b' \cup c')$. Construir tablas de propiedades de cierre para cada una. ¿Qué se puede concluir?

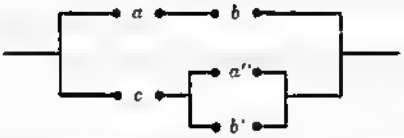
49. Hacer diagramas de cada una de las redes siguientes:

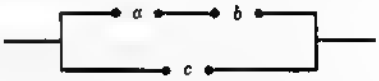
(i) $(a \cup b') \cap (a' \cup b) \cap (a' \cup b')$ (iii) $[(a \cup b) \cap (c \cup b')] \cup [b \cap (a' \cup c')]$
(ii) $(a \cap b) \cup [c \cap (a' \cup b')]$ (iv) $(a \cap b \cap c) \cup a' \cup b' \cup c'$

Mediante los resultados del Problema 30, hacer el diagrama de la red más simple en cada caso.
Respuesta parcial.

(i) 

;

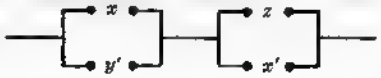

(ii) 

;


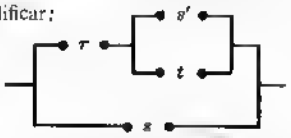
50. Hacer el diagrama de las redes $(r \cup s') \cap (r' \cup s)$ y $(r \cap s) \cup (r' \cap s')$ y mostrar que tienen las mismas propiedades de cierre.

51. Hacer el diagrama de la red más simple que tenga las propiedades de cierre de cada una de las F_1-F_6 del Problema 41.
Respuesta parcial.

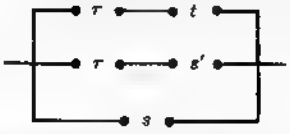
F_2 

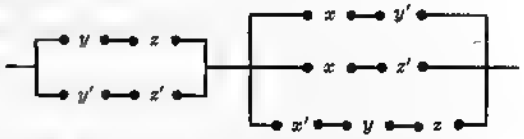
;
F_6 

52. Simplificar:

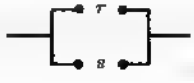
(i) 

(iii) 

(ii) 

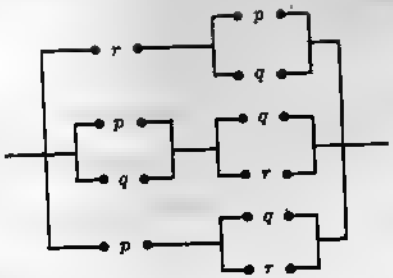
(iv) 

Para adquirir práctica y también para comprobar los resultados, se sugiere que (iii) y (iv) se resuelvan formando la tabla de propiedades de cierre y también por el procedimiento del Ejemplo 7, página 226.

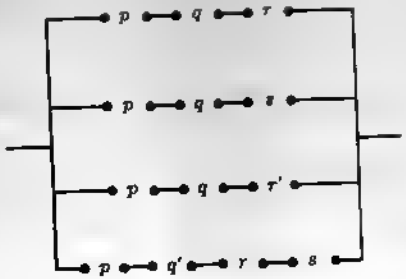
Respuesta parcial. (i) y (ii) 

53. Simplificar:

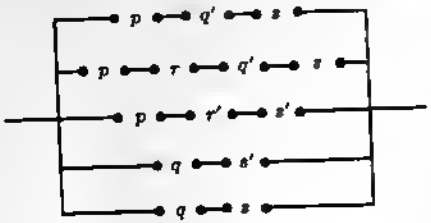
(a)



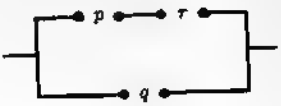
(b)



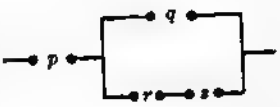
(c)



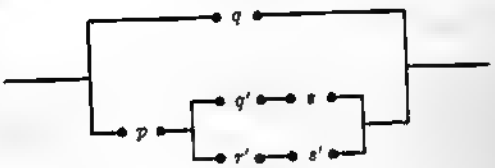
Resp. (a)



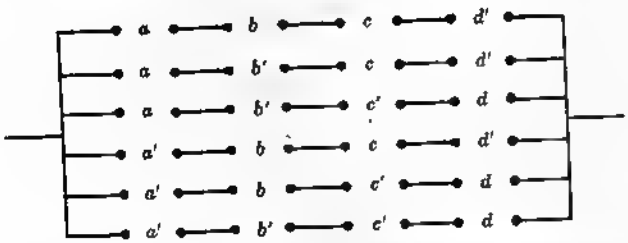
(b)



(c)



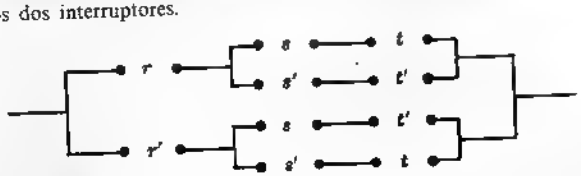
54. Simplificar:



55. Mostrar que la red del Problema 50 permite apagar o encender la luz de una escalera desde arriba o desde abajo de la misma.

56. Desde su garaje, M puede entrar a una de dos alcobas. Obtener la red que permita a M apagar o encender la luz del garaje, bien desde el garaje o bien desde una de las alcobas independientemente de las posiciones de los otros dos interruptores.

Resp.



57. Diseñar una red que permita accionar una luz desde uno cualquiera de cuatro interruptores.

INDICE

Indice de símbolos

Indice de símbolos

Schaum

3 000102 609665

• Este libro, dedicado al estudio de sistemas algebráicos, tiene por fin, servir de complemento a los textos corrientes, o bien ser utilizado como texto, por sí solo, en cursos de álgebra abstracta moderna a nivel medio superior.

• En los dos primeros capítulos, se trata de los componentes fundamentales de los sistemas algebráicos —conjuntos de elementos, relaciones, operaciones, aplicaciones—. En el capítulo 3, comienza con los postulados de Peano para los números naturales y se completa con la deducción de sus propiedades más sobresalientes.

• El primer sistema algebráico —el grupo— se estudia en el capítulo 9; se examinan las clases laterales según un subgrupo, los subgrupos invariantes y sus grupos cocientes; y el capítulo termina con el Teorema de Nordan-Hölder para grupos finitos.

• Los capítulos 10 y 11 tratan de los anillos, dominios de integridad y cuerpos. A continuación, en el capítulo 12 se estudian los polinomios sobre anillos y cuerpos a la vez que algunos conceptos de la teoría elemental de ecuaciones. En el capítulo 13 se trata el tema de los espacios vectoriales, en el 14 se trata el álgebra de las transformaciones lineales en un espacio vectorial de dimensión finita, que conduce naturalmente, al álgebra de matrices. en el 15 se tratan los polinomios de matrices como un ejemplo de anillo de polinomios no conmutativo. En el 16 se definen formalmente las álgebras lineales. En el capítulo final se exponen las álgebras boolianas y se indican las importantes aplicaciones que tienen en circuitos eléctricos simples.

9 789684 229174
ISBN: 968-422-917-8

Mc Graw Hill

ISBN 968 422 917 8